Commonwealth of Virginia

Year 2000 Assessment

October 14, 1997

Gartner Group: Executive Edge Series

Prepared for:

Joint Legislative Audit and Review Commission

Table of Contents

1. Executive Summary 1

Background

Methodology

Findings

Conclusions and Recommendations

2. Project Information 16

Background

Methodology

3. Findings: Business Issues 23

Business Profile

Business Risk Areas

Table of Contents *(Cont'd)*

4. Findings: Resource Estimates 28

Resource Estimates: Introduction

Personnel Resources: Application Repair

Exposure Analysis: Application Repair

Cost Estimate: Application Repair

Cost Estimate: Package Replacement

Cost Estimate: Computing Infrastructure

Cost Estimate: Missing Elements

Cost Estimate: Total Cost

5. Findings: Application Compliance 46

Application Compliance: Introduction

Application Compliance: Degree of INSPECTion

Compliance Strategies: Tactical Options

Compliance Strategies: Contingency Plans

Compliance Strategies: The Commonwealth Profile

Table of Contents *(Cont'd)*

4. Findings: Resource Estimates 28

Resource Estimates: Introduction

Personnel Resources: Application Repair

Exposure Analysis: Application Repair

Cost Estimate: Application Repair

Cost Estimate: Package Replacement

Cost Estimate: Computing Infrastructure

Cost Estimate: Missing Elements

Cost Estimate: Total Cost

5. Findings: Application Compliance 46

Application Compliance: Introduction

Application Compliance: Degree of INSPECTion

Compliance Strategies: Tactical Options

Compliance Strategies: Contingency Plans

Compliance Strategies: The Commonwealth Profile

Table of Contents *(Cont'd)*

4. Findings: Resource Estimates 28

Resource Estimates: Introduction

Personnel Resources: Application Repair

Exposure Analysis: Application Repair

Cost Estimate: Application Repair

Cost Estimate: Package Replacement

Cost Estimate: Computing Infrastructure

Cost Estimate: Missing Elements

Cost Estimate: Total Cost

5. Findings: Application Compliance 46

Application Compliance: Introduction

Application Compliance: Degree of INSPECTion

Compliance Strategies: Tactical Options

Compliance Strategies: Contingency Plans

Compliance Strategies: The Commonwealth Profile

Table of Contents *(Cont'd)*

5. Findings: Application Compliance *(Cont'd)*

Compliance Project Phases: Introduction

Compliance Project Phases: Repair Characteristics

Compliance Project Phases: Redeploy Characteristics

Compliance Project Phases: Reconcile Characteristics

Compliance Project Phases: Replace Characteristics

Compliance Project Phases: Retire Characteristics

Compliance Priority Plan: Introduction

Compliance Priority Plan: The Commonwealth Systems

6. Conclusions and Recommendations …….. 64

Conclusions and Recommendations

Table of Contents *(Cont'd)*

Appendices

A. Interview Participants 77
B. Agency and Institution Information 75
C. Competing Initiatives 81
D. Project Management Supplemental Information 90
E. Compliance Testing Supplemental Information 95
F. Tools and Vendors Supplemental Information 104

1. Executive Summary

Background

The Commonwealth of Virginia (the Commonwealth) recognizes that January 1, 2000 is more than just a change in the century and the millennium; it is a major challenge for nearly all its information technology (IT) systems.

In an effort to quantify its risks, the Commonwealth mandated a study of the Commonwealth's Year 2000 (Y2K) compliance in Item 14 of the Appropriations Act and assigned responsibility for this study to the Joint Legislative Audit and Review Commission (JLARC) in early 1997. The mandate stated: "(T)he Commission shall include in its study an assessment of the current status of agency actions associated with computer hardware and software problems related to the year 2000. The Commission's assessment shall include, but not be limited to, an inventory of actions completed or in progress in each agency and institution of higher education, the cost of completing all necessary modifications to hardware and software, and potential mechanisms for funding the identified costs."

The Study Issues were:

- What is the status of Y2K compliance in each state agency and institution of higher learning?
- What will it cost to modify or replace agency and institution systems to ensure Y2K compliance?
- What sources of funding, including federal and other special funds, are available to pay for necessary modifications or replacements?

The Commonwealth of Virginia, through JLARC, engaged Gartner Group, the leading global IT research, advisory, benchmarking and consulting company, to provide answers to these questions.

Methodology

Gartner Group's analysis covered the Commonwealth's IT infrastructure and application portfolio, with a particular focus on 29 state agencies and institutions of higher education. The scope includes:

- In-house and vendor-developed applications
- The Commonwealth's computing infrastructure (operating systems and major subsystems).

Gartner Group utilized a structured methodology to determine the overall costs and risks to the Commonwealth as a result of the Y2K problem. The major components of this methodology are:

- Year 2000 Exposure Analysis conducted by Real Decisions, a Gartner Group company, which quantifies the cost to repair in-house-developed applications and the relative risk in achieving that goal, based on an application inventory
- Structured interviews with IT managers in 10 key agencies and institutions to sample key processes and priorities, as well as the linkage to supporting technologies
- Shorter follow-up interviews with managers in 20 agencies and institutions to confirm and clarify reported data
- Research and interviews with Gartner Group research analysts to incorporate the most current information in this rapidly changing subject area (note: the rate of change continues to increase and is expected to increase substantially into the year 2000)
- Quantitative and qualitative analysis of the Commonwealth data
- Synthesis of results and recommendations.

Findings

Gartner Group calculated cost estimates for the Commonwealth to resolve the Y2K problem completely. It is critical to remember the following when interpreting these estimates:

- Gartner Group's estimates are based on IT industry averages applied to the Commonwealth's technology inventory, not a physical analysis of each application and operating platform (a prohibitively time-consuming and expensive task).
- Gartner Group's estimates are based on current Commonwealth cost factors. Research and experience is showing a significant drain on in-house and service vendor personnel resources to address the Y2K problem. This shortage is expected to become acute within the next six to 12 months. The supply shortage will continue to increase the cost of IT and non-IT resources.
- Some costs may be mitigated through retirement, replacement or failure strategies.
- The cost estimates represent only the prorated costs to address the Y2K problem and do not, for example, include the expenditures related to software purchases, leases or upgrades that the Commonwealth would also incur to implement a replacement strategy.
- The cost estimates represent the effort and resources that can be attributed to solving the Y2K problem. Some of these costs are already accounted for in existing Commonwealth IT budgets and future spending plans. Gartner Group experience indicates that a significant portion of these costs fall outside current budgets and spending plans.

Findings *(Cont'd)*

Gartner Group estimates that the Commonwealth will spend between $80.2 million (best case scenario) to $83.7 million (worst case scenario) for all Y2K-compliance activities associated with its statewide business application portfolio and the underlying computing infrastructure. These costs are comprised of:

Technology Area	Cost ($000) Worst Case	Best Case
Applications to be repaired	$31,070	$31,070
Applications to be repaired by contractors	$840.6	$840.6
Applications to be replaced	$8,943	$8,943
Computing infrastructure	$28,889	$28,889
Risk factor	$13,949	$10,461
Total	$83,692	$80,204

This cost estimate is based upon a fully burdened cost per application support person of $78,000 per year (comprised of compensation, benefits, system and facilities costs). This figure is in line with the average cost for all governmental units, but it is approximately 29 percent below that of all organizations.

The risk factors take into account the fact that the number of business applications will grow as application inventories are completed and that the hardware inventory provided to Gartner Group documents a number smaller than that stated by the Council on Information Management (CIM) in earlier years. These are conservative risk factors based on the degree of missing data and the unknowns about future cost escalation.

Findings *(Cont'd)*

In addition, Gartner Group has identified the following Y2K problem risk areas (note: Gartner Group's expertise is in the IT arena, but, where appropriate, it has also documented non-IT issues that were revealed as a part of this study):

- The Y2K effort within the Commonwealth has been structured as a confederation of separate projects, rather than as a cohesive, planned effort. The Commonwealth would benefit from the establishment and empowerment of a true project office whose authority would extend well beyond that of the statewide coordinator now working to harness the efforts of these agencies and institutions. While the statewide coordinator now in place has done a good job in gathering data, more is needed.
  - Project management is critical, and creating an effective program office is key to success. The core program management office should be a statewide team, with authority for review and audit of agency and institution project plans and schedules, and final sign-off on testing compliance certification results. There must be one leader of the program management office charged with statewide compliance. A hierarchy should be built under the core team as needed, centrally and within the agencies and institutions.
  - The Commonwealth would benefit from the use of common project templates, the establishment and enforcement of certain timelines, and other elements of world-class project management,
  - The Commonwealth's considerable IT infrastructure can be used to facilitate testing. With nine available mainframes, the Commonwealth need not rely on one central machine for testing purposes. In addition, available midrange resources must be identified and put to work in testing.

Findings *(Cont'd)*

Year 2000 problem risk areas *(Cont'd)*:

- There is great reliance on replacement as a means of addressing the Y2K problem in the Commonwealth. It is very important to weigh the risks of replacing applications with vendor packages against the benefits of this strategy, and that achievable plans are in place for these efforts.
- There has been relatively little detailed planning with regard to the testing and compliance elements of the Y2K project. This focus on the initial elements of the process is understandable, but the crucial latter stages must be addressed promptly to ensure that the Commonwealth's systems are fully compliant.
- There is little evidence of a "supply chain" view of the Y2K problem in the Commonwealth. What is in evidence is an IT-centric focus on systems. It is highly important for the agencies and institutions of the Commonwealth to map their information flows, determine other organizations on which they might rely and contact external providers to query their Y2K compliance level.
- There is evidence of a lack of ability to discern among levels of importance of applications: Nearly all applications identified in this study were given mission-critical status. As a result, the decisions that may have to be made if triage becomes a reality remain to be made, and there is little evidence of a framework in which this decision will occur. This rigorous questioning and priority-setting process should be a basic responsibility of the statewide project management office.

Findings *(Cont'd)*

Year 2000 problem risk areas *(Cont'd)*:

- The Commonwealth's telecommunications services demand additional focus. The Commonwealth receives services both from internal staff and external providers. Of particular concern are the PABXs and other time- and date-sensitive devices supporting its voice network, and the hubs, routers and other time- and date-sensitive devices supporting its data network of more than 2,200 data circuits. The Y2K project for its telecommunications infrastructure will mirror that of the overall IT project, with a requirement both of internal staffing and capability analysis and intense vendor management.
- Gartner Group's interviews indicate that the potential Y2K problems associated with other non-IT technologies (e.g., security systems, environmental control systems, elevator control systems) are generally not understood or being addressed. There must be communication and technology transfer between IT and non-IT professionals on the steps in addressing Y2K concerns, with particular emphasis on the vendor management process.
- Certain agencies and institutions face larger risks primarily because of staffing shortages. In Gartner Group's analysis, fully 50 percent of the reporting agencies and institutions reported staff shortages. To a lesser extent, there were risk flags for staff turnover and limited staff tenure. The largest obstacles mentioned to meeting the demands of the Y2K project in the context of meeting key business demands were the lack of qualified personnel and lack of adequate funding.

Findings *(Cont'd)*

Year 2000 problem risk areas *(Cont'd)*:

- While there had been relatively little loss of staff as a result of offers from the private sector, what the interviewees reported was increasing difficulty in finding personnel qualified in older systems. More than one interviewee expressed the concern that the agency's reliance on contractors made the underpinning of the Y2K project uncertain.
- Some IT organizations may be experiencing a false sense of security because individual applications are Y2K-compliant. These organizations are only approaching the most difficult and demanding phase of Y2K compliance, which is integration testing. In this phase, the internal linkages between a business unit's applications as well as the interfaces to external business partners must be tested and modified. This phase is completed only after a rigorous audit or certification process has been completed.
- There was little evidence of explicit budgeting for Y2K projects having been performed by these agencies and institutions. Furthermore, Gartner Group has found no evidence of special federal funds planned for use by state or other government agencies for addressing this problem.
- There was a distinction drawn between generally funded and specially funded agencies in their outlook on funding prospects. The former were particularly concerned about the relatively limited size of the Special Loans Fund; they were further concerned about the Fund's status as a *loan* vs. an appropriation fund. The latter generally sensed no real limitations on funding.

Conclusions and Recommendations

Based on the data supplied for this study, the Commonwealth's outstanding cost to achieve Y2K compliance for its IT applications and computing infrastructure will range from $80.2 to $83.7 million. A key factor in this calculation is the Commonwealth's estimate of a uniform annual cost per person (see the following page for assumptions).

Because of several important factors, the total cost of the Commonwealth's Y2K project is likely to grow beyond this figure. These factors are:

- The Commonwealth's need to rely on external contractors for its remediation and testing work
- The number and magnitude of software packages and hardware platforms not now in the Commonwealth's inventory
- The magnitude of cost required for non-IT assets.

Conclusions and Recommendations *(Cont'd)*

Analysis reveals the following key cost drivers:

- Personnel cost: The total cost of achieving Y2K compliance is calculated using the Commonwealth's fully loaded (compensation, benefits, supporting systems) cost per person. This cost estimate is based upon a fully burdened cost per application support person of $78,000 per year (comprised of compensation, benefits, system and facilities costs). This figure is in line with the average cost for all governmental units, but it is approximately 29 percent below that of all organizations. It is likely that, as a result of the Commonwealth's broadening of the range of allowable "body shop" relationships and because of the growing demand for qualified resources, the total cost per person of Y2K work will rise toward Gartner Group's average cost level. The cost of the Commonwealth's Y2K project, calculated at this average, would today exceed $115,000,000.
- Size of application portfolio: The Commonwealth's application portfolio is largest in the groupings (government units, database average, eastern U.S. companies and large companies) represented in this study. The current Gartner Group database is comprised of 85 organizations, although Gartner Group has performed approximately 500 application benchmarks since 1990. This positioning is caused by the number and diversity of the Commonwealth's units and their relative homogeneity. As a result, there is relatively little opportunity to create either specialty reuse centers or project management competency center(s). Each group believes that it is in large measure on its own in addressing its Y2K problems. The project has been made that much more complicated by this factor.
- Productivity: Gartner Group's analysis indicates that the Commonwealth's application support productivity is higher than average, but in line with that of government entities in general.

Conclusions and Recommendations *(Cont'd)*

The Y2K problem is matter of survival, not just an IT problem. While the challenges facing the Commonwealth's IT organizations are substantial, the Commonwealth must also begin immediately to address supply chain (suppliers and customers) and non-IT infrastructure issues. As a result, Gartner Group recommends that the Commonwealth:

- Immediately strengthen the central Y2K project office commissioned by the Commonwealth. There must be a core staff of IT and non-IT personnel dedicated to this effort. The project office must leverage the experience of the Commonwealth's Y2K problem "centers of excellence" quickly to disseminate best practices and to leverage tools and techniques. Gartner Group's interviews suggest, for example, that the University of Virginia may be a center of excellence in terms of Y2K planning and organization.
- Empower the project office to set statewide standards and prioritize plans to address the Commonwealth's business applications, IT infrastructure, telecommunications infrastructure, process control systems and supply chain interfaces. These plans must address staffing, service vendor and funding requirements as well as business and IT contingency options.
- Prioritize Y2K compliance efforts. Refine the Commonwealth's application prioritization scheme to ensure that the largest and most business-critical applications are accurately identified. Focus repair efforts on the largest and most critical applications. Gartner Group's analysis indicates that the Commonwealth's Y2K project efforts have been focused primarily on process-important applications and on its infrastructure to date. Progress on mission-critical and mission-important applications is lagging; there is also much work to be done on process-critical applications. The need to redirect focus may well lead to an acceleration of cost.

Conclusions and Recommendations *(Cont'd)*

- Gartner Group further recommends that the Commonwealth's Project Management Office:
- Ensure that the Commonwealth monitors compliance progress based on application priority. A critical element of this priority ranking must be the potential legal liability of Y2K failures, particularly in the Department of Corrections and in Medical Assistance Services, and in other areas open to litigation involving entitlements and constitutional rights.
- Establish a Y2K-compliance certification program for the Commonwealth's agencies and institutions and their supply chains.
- Begin an active communication campaign to raise Y2K awareness within the end-user and IT developer communities. Provide guidelines as well as conversion and testing assistance as needed for high-impact systems.
- Extend this communication campaign outside of IT. There was a question among the agencies and institutions interviewed whether there was real focus on the Commonwealth's Y2K problem on the part of decision-makers in state government, particularly in light of the fact that 1997 is an election year.
- Work to develop personnel retention policies and plans, including both financial incentives and targeted management attention. The current plan to provide a cumulative bonus of $10,000 over the balance of the century was deemed insufficient to retain critical personnel. Training commitments can also be used to the Commonwealth's benefit.

Conclusions and Recommendations *(Cont'd)*

- The Commonwealth's Project Management Office should also:
- Maintain focus of the Commonwealth's leadership on the Y2K problem and its implications.
  - There were expressions of concern about the amount of incremental unexpected work that would arise as a result of new legislation in the session commencing January 1998. This concern must be analyzed and supported, if appropriate.
  - There was more than one request for a freezing of legislative mandates during the coming session, in order to allow the agencies and institutions to follow through on making the Y2K problem their highest priority. This position must be analyzed and supported, if appropriate.
- Ensure that the Commonwealth's leadership recognizes that the "rules of the game" are changing increasingly rapidly, which means:
  - Funding requirements are likely to change over time
  - New service vendor offerings and tools are appearing on a regular basis
  - Ongoing access to current Y2K information, best practices and experts is essential.

Conclusions and Recommendations *(Cont'd)*

The Commonwealth's agencies and institutions must:

- Recognize that there are a number of risks associated with package replacement strategies:
  - Qualified implementation vendor resources are becoming increasingly scarce
  - Package implementation may require significant changes to business processes
  - The Commonwealth will need to rely on vendor warranties and reputation to ensure Y2K compliance.
- Understand that the testing phases are particularly time-consuming and demanding of project management skills. There has been relatively little detailed planning with regard to testing and compliance elements of the Y2K project. These crucial latter stages must be addressed promptly to ensure that the Commonwealth's systems are fully compliant. Furthermore, the Commonwealth's agencies and institutions must be aware of their need to conduct testing on midrange platforms.

Generally, the Commonwealth should be careful when comparing its results to those of other states, keeping the following points in mind:

- Different states are at different points in dealing with the problem.
- The results reported by each state must be normalized based on the size and nature of the application inventory as well as the size of the state.
- The methodology used to develop the other estimates must be understood, since other states may have internally underestimated the cost to address the Y2K problem fully.

2. Project Information

Background

The Commonwealth of Virginia is not unique in facing significant challenges to addressing the Y2K problem. This problem is the result of technology design and programming practices that represent the year component of dates as two, rather than four, digits (for example, “97” instead of “1997”). The result of this date representation can lead to incorrect calculations and decisions that are based on dates. The impact of these technology errors can range from annoying to catastrophic. The business impact of each potential technology failure must be understood in order to ensure that appropriate resources are committed to fixing the problem.

The various IT organizations across the Commonwealth’s agencies and institutions have addressed the Y2K problem to varying degrees. However, one of the biggest obstacles to solving the Y2K problem is viewing it strictly as an IT problem. The following excerpt from a recent Gartner Group research paper (*Year 2000 Compliance Implementation: Organizing for Success: R-Y2K-102*) highlights this point:

- “The Y2K project is viewed as hype and treated with derision in many application development (AD) organizations. IT staff members closest to the IT portfolio at risk have often been rebuffed in their efforts to raise management awareness of the problem. Since the problem is viewed as a “mainframe” problem (indeed, more than 75 percent of the affected code is COBOL), it can be extremely difficult to find resources willing or able to work on the project, as legacy systems are not viewed as strategic in the eyes of most upwardly mobile IT professionals. In many cases, the Y2K task is viewed as a boring maintenance effort akin to washing ashtrays.”

Background *(Cont'd)*

The article continues several paragraphs later:

- "The Y2K challenge rises above the problem level for several reasons:
  - It will touch every system, every technology, every application and every tool in the inventory, and may affect the long-term management of these technologies.
  - It will likely consume more resources than any other IT project in the past.
  - It requires inter-business-unit and inter-enterprise political navigation.
  - It must be managed and prioritized skillfully, since resources probably are not available to fully complete it.
- Obtaining (and retaining) the best people begins by viewing the Y2K project as a bet-the-business disaster avoidance effort, rather than as a software maintenance effort. This is easier to understand when it is brought to light that 90 percent of all software applications are likely to fail if not corrected for the Y2K problem (0.8 probability). Those that work on the problem are playing critical roles in keeping the enterprise's IT infrastructure functioning, and thus in saving the business. The highest levels of management must acknowledge this importance."

Methodology

Gartner Group utilized a structured methodology to determine the overall costs and risks to the Commonwealth as a result of the Y2K problem. The major components of this methodology are:

- Year 2000 Exposure Analysis
  - Conduct an application inventory: Collect data on the Commonwealth's major applications including lines of code (LOC) by language, database methods and sizes, number of users, application priorities, Y2K compliance strategies (see *Methodology: Application Inventory Priorities* for definitions)
  - Calculate the size of the application portfolio, in terms of function points, then estimate the cost to repair the portfolio, based on the Commonwealth's productivity and cost structure
  - Analyze the Commonwealth's application support staffing: personnel levels, turnover, and tenure
  - Determine the Commonwealth's relative risk in repairing the portfolio, based on the aggregate risk factors.

Methodology

- Structured interviews
  - Identify key individuals with an understanding of both the Commonwealth's priorities and issues as well as those of their own agencies/institutions, and an appreciation of the linkages to underlying technologies and applications
  - Provide an interview guide to prepare the Commonwealth interview participants
  - Conduct in-person and audio/videoconference interviews to surface significant issues related to the Y2K problem at the Commonwealth
  - Capture results electronically and analyze responses.
- Research and additional interviews
  - Review existing Gartner Group research in areas of special relevance to the Commonwealth, for example, best practices related to supply-chain compliance
  - Review other publicly available research and documentation in areas of special relevance to the Commonwealth
  - Interview Gartner Group research analysts specializing in matters related to the Y2K problem in areas of special relevance to the Commonwealth, for example, personnel retention policies.

Methodology *(Cont'd)*

- Quantitative and qualitative analysis of the Commonwealth data
  - Input the Commonwealth's data into Gartner Group's analytic models and derive preliminary metrics
  - Identify and reconcile or resolve any data anomalies with the Commonwealth, as appropriate
  - Make final the quantitative analysis.
- Synthesis of results and recommendations
  - Conduct peer review of findings
  - Document findings and recommendations
  - Review and refine with the Commonwealth and Gartner Group project team.

Methodology: Application Inventory Priorities

For each application system, the project teams of each of the Commonwealth's identified agencies and institutions assigned one of the following application priorities:

- **Mission Critical:** Priorities directly affect the customer and the revenue stream. The loss of a mission-critical application for a period of time leads to non-recoverable consequences
- **Mission Important:** The agency may recover from some downtime to a mission-important application.
- **Process Critical:** Priorities directly affect the building of the agency's services, though not directly visible to the customer. The loss of a process-critical application leads to non-recoverable consequences.
- **Process Important:** The agency may recover from some downtime to a process-important application.
- **Infrastructure:** Helps run the internals of the agency. A period of downtime is usually recoverable.
- **Reporting:** Provides information necessary to run the agency, but downtime has only internal consequences.

These business-based definitions were adapted by respondents to correspond to their activities.

3. Findings: Issues

The Commonwealth's Profile: Implications

The Commonwealth's profile, as revealed by sample interviews, indicate areas of potential advantages and disadvantages for addressing the Y2K problem:

- **Stature:** The Commonwealth should enjoy significant economies of scale as a large customer as well as preferential treatment as a showcase customer from key IT and non-IT suppliers. These economies of scale can emerge only with the centralized planning and execution of a strong project management office.
- **Decision-making:** The Commonwealth is comprised of 90-100 largely autonomous agencies and 30-40 institutions of higher education. The significant decentralization of decision-making creates a potential cultural impediment to the information sharing and centralized decision-making that will be necessary to address the Y2K problem expeditiously.
- **Diversity:** The Commonwealth has a heterogeneous assortment of IT and non-IT assets that are critical to its various agencies and institutions, and which must be analyzed individually for Y2K compliance. This technological diversity will require greater effort to resolve the Y2K problem than a standardized, homogenous environment.
- **Risk tolerance:** The Commonwealth generally has a risk-aversive culture. This risk aversion indicates a preference for longer test periods and buffer zones (time period prior to technology failure) in order to achieve end-user acceptance than may actually be available before the advent of the year 2000.

Issues: Risk Areas

Gartner Group conducted structured interviews with IT managers in ten agencies and institutions to sample key processes and priorities. The following Y2K problem risk areas were identified as a result of these sessions. Because of the relatively small sample size and the technology orientation of the interviewees, the following are meant to be indicative, not comprehensive, observations. Also, Gartner Group's core expertise is in the application of general-purpose information technology to solve business needs, but it also recognizes that the Y2K problem has significant non-IT implications that must be identified and addressed by the Commonwealth.

Following are key issues identified by Gartner Group:

- Gartner Group's interviews indicate that the potential Y2K problems associated with non-IT technologies (e.g., telephone switches, data networks, security systems, environmental control systems, elevator control systems) are generally not understood or being addressed. There is little or no communication and coordination between IT and non-IT personnel.
- The most expeditious solutions to the Commonwealth's Y2K problem will require a centralized approach, taking calculated risks, that is contrary to the Commonwealth's current culture. The danger is that this cultural dissonance will increase the time involved in addressing the Y2K problem.
- A number of agencies and institutions report large numbers of competing initiatives over the coming three years: This overburdening of staff calls into question the level of priority being given the Y2K imperative, and it leads to concerns whether any of the major initiatives will be achieved. A table of competing initiatives may be found in Appendix.

Business Issues: Risk Areas

- Certain agencies and institutions face larger risks because of staffing shortages (Y2K staffing is more than 50 percent of current staff). Staff turnover (more than 25 percent in the last year) is an important second risk factor. Limited staff tenure (average less than three years) did not emerge as a serious risk factor for the Commonwealth.
  - Staff shortage (50 percent of agencies included in this study): Department of Accounts; Alcoholic Beverage Control; Community College System; Department of Corrections; Board of Elections; Employment Commission; George Mason University; Department of Juvenile Justice; Department of Medical Assistance Services; State Police; State Corporation Commission; Department of Taxation; Virginia Commonwealth University; Virginia Tech.
  - Staff turnover (29 percent of agencies and institutions included in this study): Alcoholic Beverage Control; Department of Corrections; Lottery Commission; Department of Medical Assistance Services; Old Dominion University OCCS; Department of Taxation; University of Virginia; Virginia Commonwealth University.
  - Low tenure: State Corporation Commission.
- Those agencies with two risk factors (Alcoholic Beverage Control; Department of Corrections; Department of Medical Assistance Services; State Corporation Commission; Department of Taxation; and Virginia Commonwealth University) will bear special attention.

Business Issues: Risk Areas *(Cont'd)*

- Some IT organizations may be experiencing a false sense of security because individual applications are Y2K-compliant. These organizations are only approaching the most difficult and demanding phase of Y2K compliance, which is integration testing. In this phase, the internal linkages between a business unit's applications as well as the interfaces to external business partners must be tested and modified. This phase is completed only after a rigorous audit or certification process has been completed.
- The Commonwealth's agency systems appear not to have the reliance on user-developed applications that is often found in private industry. Where there are potential problems, they seemed concentrated in budgetary and planning functions (process-, not mission-related). While risks from user-developed applications seems to be under reasonable control in a number of agencies, the Commonwealth must act to ensure that such user-developed applications are identified and brought into Y2K compliance, particularly in its institutions.

4. Findings: Resource Estimates

Resource Estimates: Introduction

Gartner Group has analyzed the resources needed by the Commonwealth to fully correct Y2K problems in its statewide information technology application portfolio and related computing infrastructure. This is based on the information supplied by the Commonwealth as part of a detailed data collection process. Findings are presented regarding:

- Personnel resources: The Commonwealth's staffing requirements to address the Y2K problem were calculated based on the Commonwealth's assessment of each application's compliance; results are interpreted based on current staffing levels and staff productivity
- Exposure analysis: The degree of difficulty in repairing in-house-developed applications is based on many factors, including technological complexity, number of interfaces between systems and staff tenure; the exposure analysis indicates the Commonwealth's relative risk in successfully addressing the Y2K problem based on these elements
- Cost estimates: The Commonwealth's cost to address the Y2K problem is a combination of: 1) the personnel costs required to correct problems in existing applications developed by the Commonwealth personnel (referred to as the repair scenario in this report), 2) the *incremental* personnel and system costs required to test Y2K issues for applications to be replaced, and 3) the *incremental* personnel and system costs required to test Y2K issues in the computing infrastructure (hardware, firmware, operating system and general purpose sub-system); a range of total costs is calculated based on different assumptions regarding the Commonwealth's need to repair applications that are slated for replacement or retirement (as a precaution) and the degree of overall risk.

Resource Estimates: Introduction *(Cont'd)*

The cost and labor requirements of repairing the Y2K problem were estimated for each application in order to begin planning and budgeting for Y2K compliance. These preliminary estimates include costs for:

- Project management
- Locating and identifying affected code and data
- Parsing and analyzing affected code and data
- Determining options
- Implementing solutions
- Unit, system and integration testing
- Implementation.

The estimates do not include:

- Tool costs
- Machine resources
- End-user acceptance
- Documentation
- Standards updates.

Resource Estimates: Introduction *(Cont'd)*

Certain charts on the following pages use codes to show how the Commonwealth compares to other companies with similar characteristics. These selected subsets of companies from Gartner Group's database are referred to as peer groups. The following codes were used in this report:

- VA The Commonwealth
- AVG Average of all organizations in the Gartner Group database
- EAS Organizations primarily located in eastern North America
- LRG Large organizations
- GOV Government entities

For many organizations, the biggest impediment to Y2K success is inadequate staffing because of:

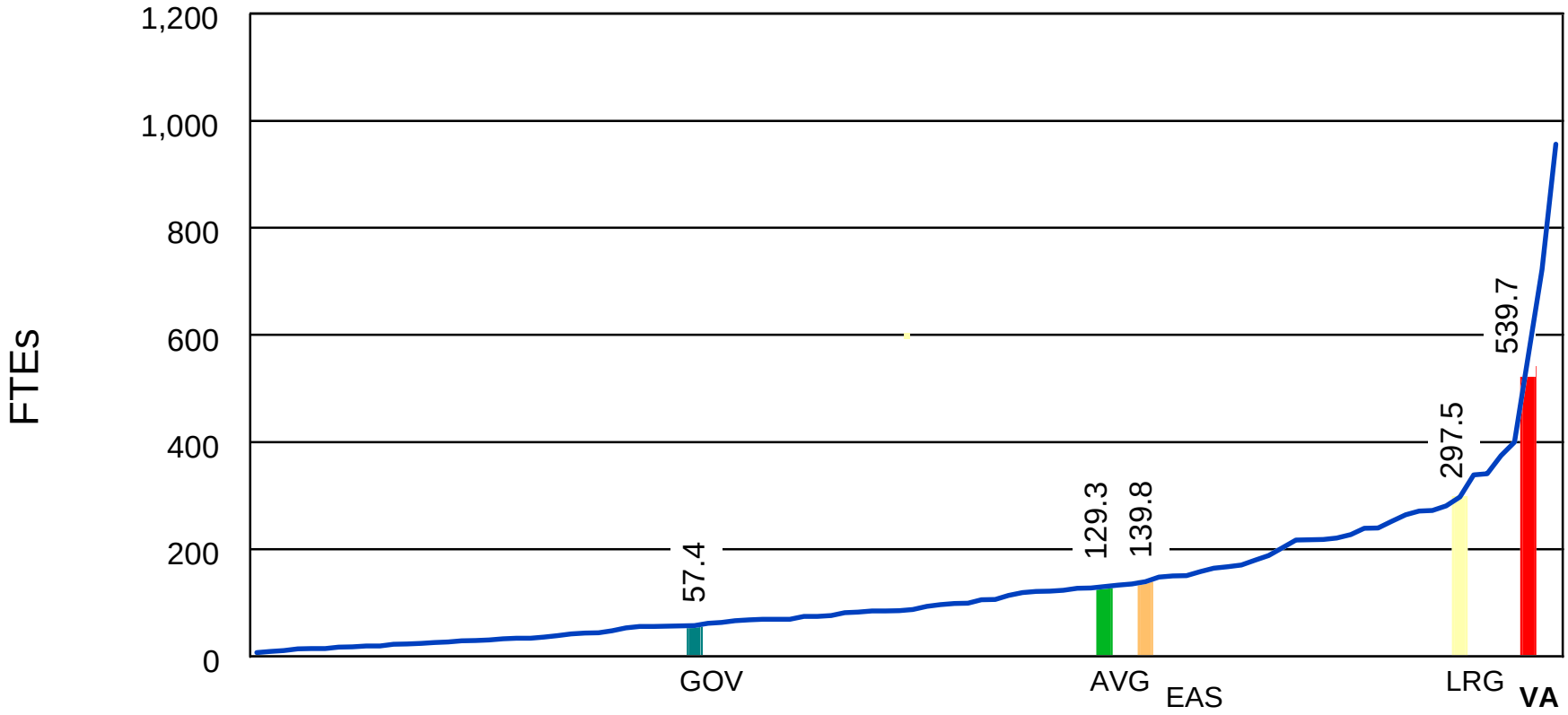
1. Staff being assigned part-time
2. Shifting priorities
3. Assignment changes to other projects.

The Commonwealth must ensure that the Y2K project teams statewide are not diverted to other projects to minimize the risk that Y2K-compliance schedules will not be met.

Personnel Resources: Application Repair

The Commonwealth's estimated FTEs required to fix the Y2K problem is largest among these groupings. This requirement is based in the large number of internally developed and maintained applications, and the heterogeneity of the Commonwealth's platforms.

Estimated Full Time Equivalents Required to Fix Year 2000 Problem (In-House-Supported Software)



Personnel Resources: Application Repair *(Cont'd)*

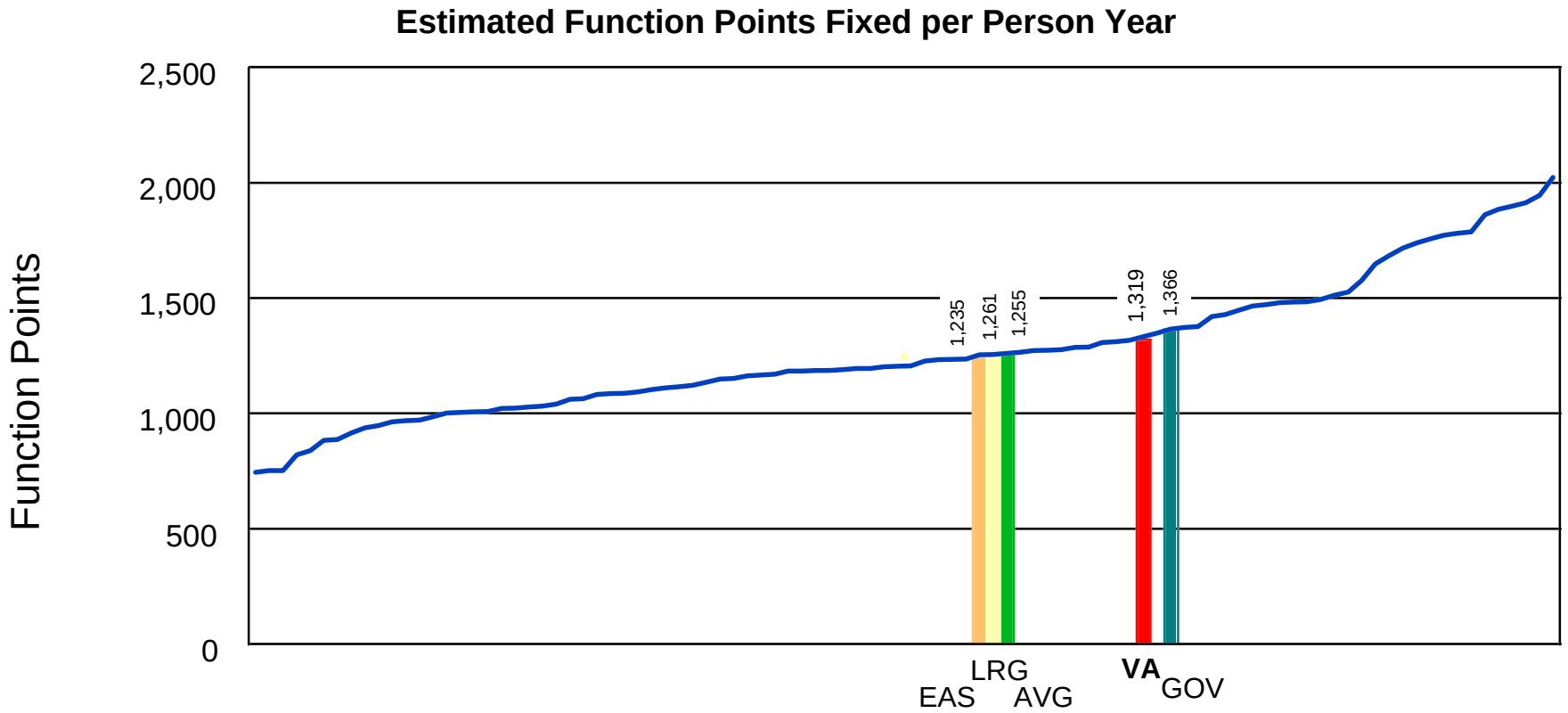
The Commonwealth's personnel requirements (FTEs) needed to repair the Y2K problem for in-house-developed or modified applications is shown below by application system priority. The total cost column shows the amount required to completely repair each application and the remaining cost column takes out the labor already expended (based on the Commonwealth's reported level of Y2K compliance by application).

Full Time Equivalents Required to Fix Year 2000 Problem

Category	Total FTEs To Repair	Remaining FTEs To Repair
Mission Critical	367.3	286.3
Mission Important	45.9	38.2
Process Critical	11.2	10.8
Process Important	33.4	22.5
Infrastructure	70.1	38.3
Reporting	2.7	2.3
Total	530.5	398.4

Personnel Resources: Application Repair *(Cont'd)*

The Commonwealth's staff productivity (function points fixed per person per year) is higher than average, driven by a combination of low exposure index, minimal functionality in low-level languages and higher percentage in 4GLs (specifically Natural, Powerhouse, Oracle, MAPPER and PowerBuilder). Productivity is estimated based on the mix of programming languages.

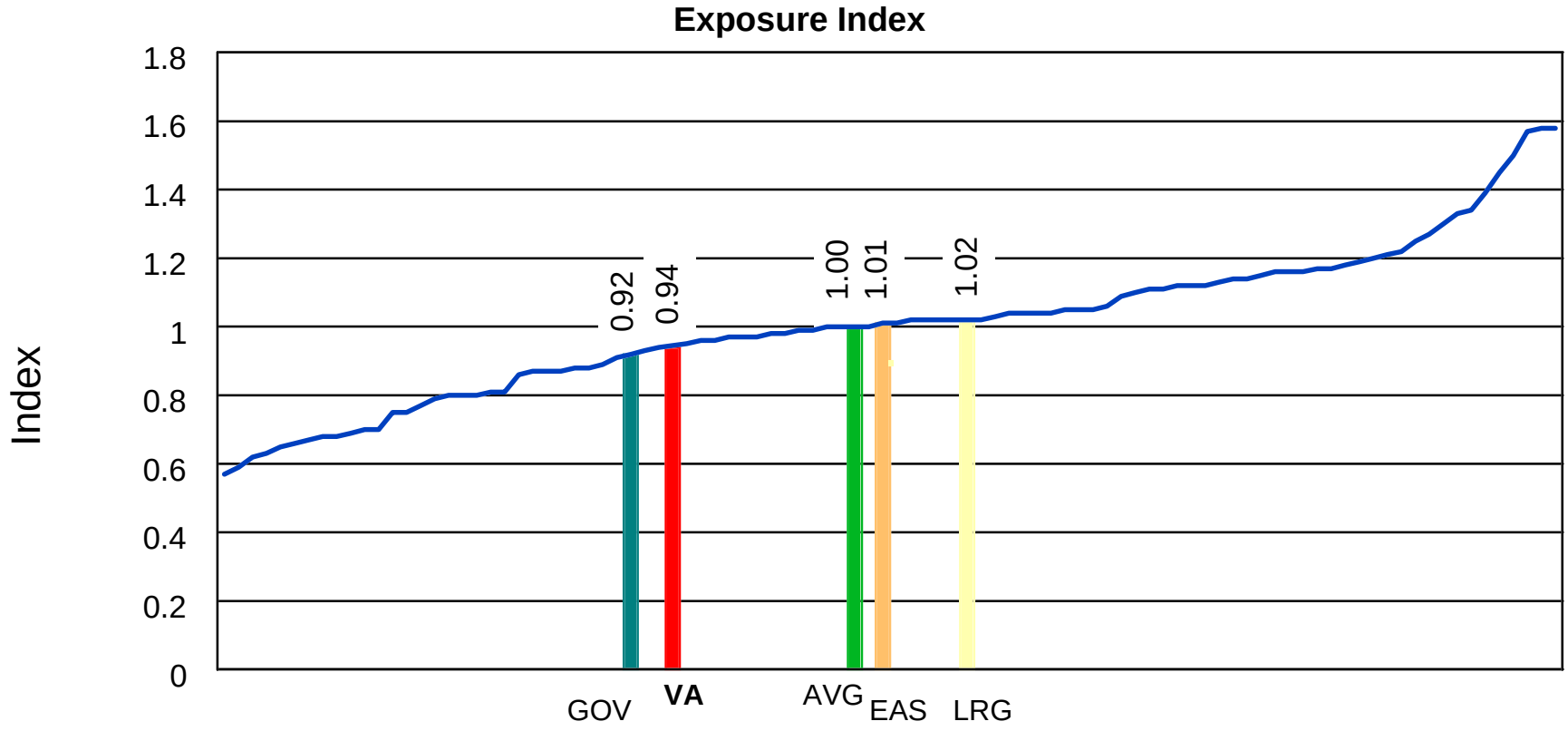


Exposure Analysis: Application Repair

Gartner Group's proprietary exposure analysis assesses the likelihood of successfully completing Y2K remediation of the in-house application portfolio. The objective is to create awareness of the general scope and risk of the project before more accurate estimates, based on the chosen methodologies and detailed work breakdown, can be developed. There is no causal relationship between the exposure index, which is a function of the application technology and support staff composition, and the total cost to repair, which is a function of the size of the application portfolio and the cost per person.

Exposure Analysis: Application Repair *(Cont'd)*

The Commonwealth's Y2K exposure index is lower than average but in line with government entities. The Commonwealth's distinguishing characteristics are: use of fourth-generation languages, which is higher than average (the Commonwealth's usage is 54 percent vs. Gartner Group database average of 36 percent); and longer-than-average staff tenure.

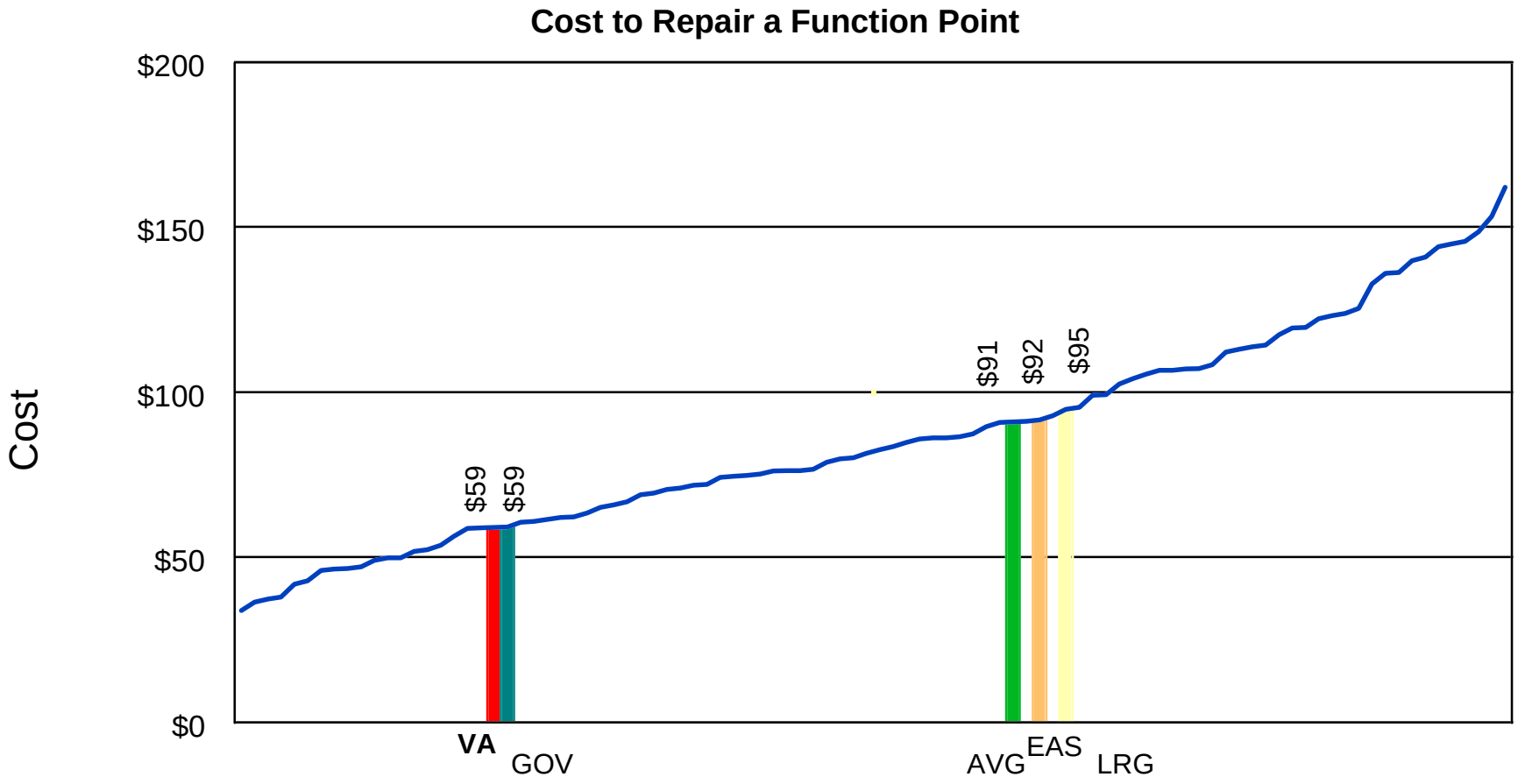


Cost Estimate: Application Repair

- Gartner Group's estimate of the cost of repairing the Commonwealth's in-house application base is based on:
  - An analysis of the number of function points in the Commonwealth's in-house application inventory (developed and modified) as well as the degree of Y2K remediation for each application (note: function points are a measure of the size and complexity of applications that is independent of the programming language(s) used to code the application. This is the most accurate means to size and compare the application portfolios of different organizations, since they are comprised of applications developed in many different languages)
  - An average cost to repair based on the Commonwealth's fully burdened cost per person, rather than on industry averages
  - The current cost structure and productivity of the Commonwealth IT application support personnel. The use of other resources (e.g., contractors, hardware, package purchases and upgrades, etc.) could increase or decrease the total cost estimate substantially.
- While the Commonwealth's Y2K remediation strategy for some key applications is to replace these applications with Y2K-compliant vendor packages, it is critical to recognize that some repair work will need to be done as a precaution, depending on the timing and risk of replacement. As a result, the true cost of remediation will fall somewhere between a worst case scenario (assumes that applications to be replaced or retired will be completely repaired) and a best case scenario (assumes that applications to be replaced or retired will require no repair effort).

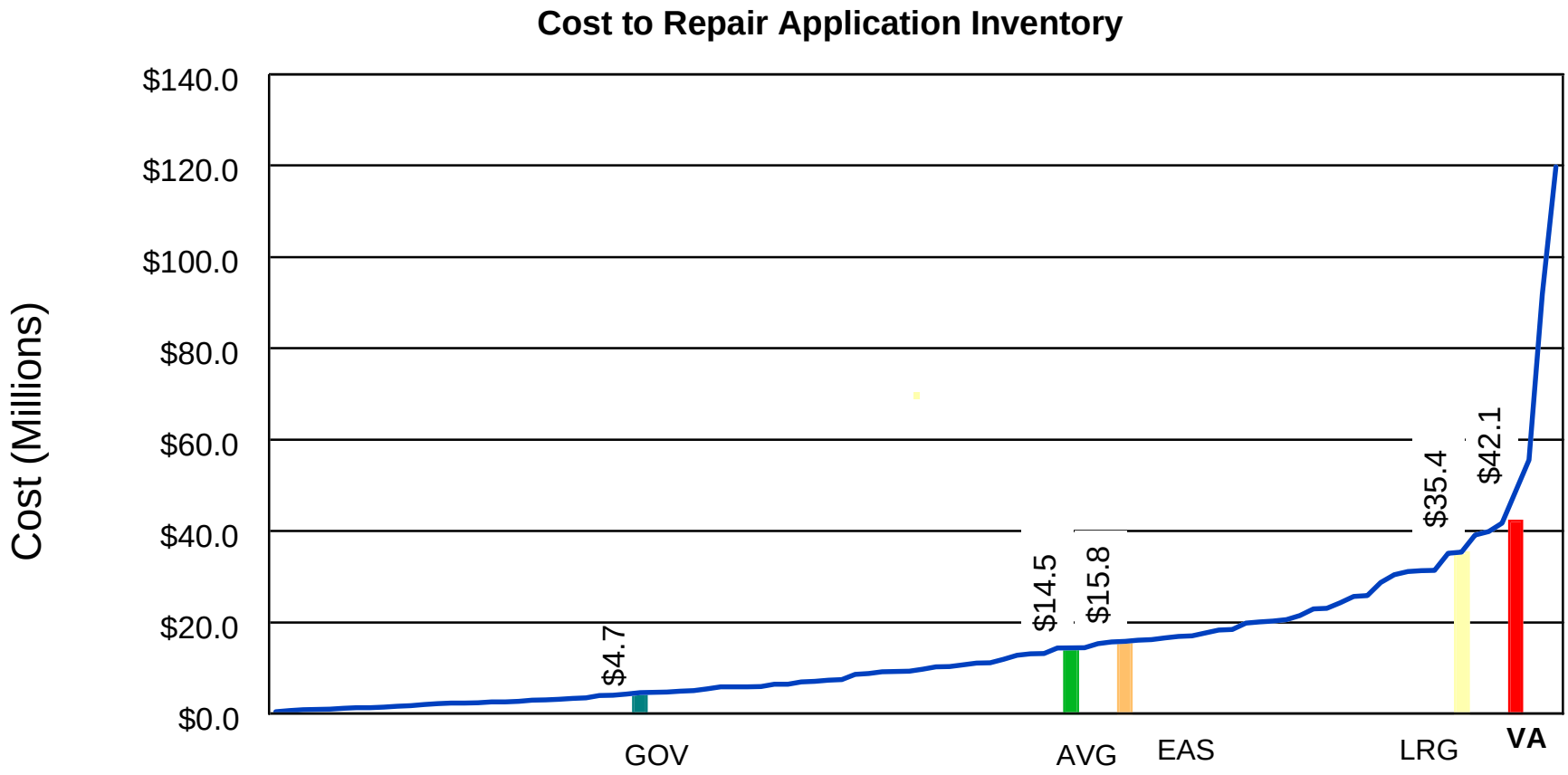
Cost Estimate: Application Repair *(Cont'd)*

The Commonwealth's cost to repair per function point is lower than average because of the lower cost per person. It is line with the average for government entities.



Cost Estimate: Application Repair *(Cont'd)*

The Commonwealth's cost to fully repair the Y2K problem for the in-house application portfolio is higher than average because of the larger-than-average size of the application portfolio.



Cost Estimate: Application Repair *(Cont'd)*

Analysis of the breakdown of the cost to repair the in-house application portfolio reveals two key findings. First, based on the Commonwealth's self-evaluation, 11 percent of the entire application portfolio has been made Y2K-compliant. Second, Process-Important applications and Infrastructure have been addressed as a priority, leaving much work to be done on applications of greater criticality.

Cost to Repair by Category

Category	Total Cost to Repair	Remaining Cost to Repair
Mission Critical	$28,646,379	$22,331,031
Mission Important	$3,576,768	$2,980,466
Process Critical	$876,947	$840,293
Process Important	$2,601,330	$1,752,038
Infrastructure	$5,466,670	$2,986,711
Reporting	$209,757	$180,429
Total	$41,377,851	$31,070,967

Cost Estimate: Package Replacement

The Commonwealth has identified nine major applications that will be replaced by software packages. The replacement option has generally been selected to satisfy one or more of the following:

- Provide additional functionality
- Move to a more standardized environment
- Stay current with vendor maintenance requirements
- Change computing platforms.

Gartner Group has developed cost estimates for the effort involved strictly with the Y2K-compliance portion of implementing or upgrading an application package. In other words, the costs associated with implementing or upgrading the non-date-related functionality and the cost of the package itself are excluded. The costs are derived from the magnitude (in terms of acquisition price) of the package. The cost estimates for replacement are comprised of the following:

- Personnel: The prorated labor costs associated with planning the Y2K component of the package implementation, conducting Y2K unit tests (including developing, running, debugging and executing test scripts, documenting successes and failures as well as performing any corrective actions, as needed) and Y2K integration testing (the same types of activities described under unit testing, but applied to interfaces with other applications and external systems)
- System: The incremental machine resources (for example, increased disk size to handle expanded dates) required to install a Y2K-compliant application package relative to a non-compliant version.

Cost Estimate: Package Replacement *(Cont'd)*

Gartner Group estimates that the Commonwealth will spend $8.9 million to make applications targeted for replacement Y2K-compliant (this is in addition to any repair efforts that will be necessary, identified previously). Detailed information for replacement follows.

Number of applications	9
Total package value ($000)	$21,700.0
Number of FTEs	87.3
Cost per FTE ($000)	$78
Personnel cost estimate ($000)	$ 6,809.4
System cost estimate ($000)	$ 2,134.0
Total	$ 8,943.4

Cost Estimate: Computing Infrastructure

The Commonwealth has a significant inventory of computers across the enterprise. There is a tremendous diversity in the application mix, processing capacities, operating environments, locations and vintages of these computers. The operating systems (such as MVS, HP-UX, Unix) and major subsystems (such as CICS, IMS) of each machine must be upgraded and tested for Y2K compliance.

Gartner Group has developed cost estimates for the effort involved strictly with the Y2K-compliance portion of upgrading to a Y2K-compliant operating environment. In other words, the costs associated with implementing or upgrading the non-date-related functionality are excluded. The costs are derived from the magnitude (in terms of acquisition price) of the operating environment. The cost estimates for computing infrastructure upgrade are comprised of the same elements as replacement (personnel and system components).

Gartner Group estimates that the Commonwealth will spend approximately $29 million to make its computing infrastructure Y2K-compliant. Detailed information by platform follows.

Computing Environment	Number	Cost ($000)
Large-Scale (mainframe) computers	9	$11,124
Medium-Scale (midrange) computers	75	$9,765
Small-Scale (servers,department) computers	200	$8,000
Total	284	$28,889

Cost Estimate: Missing Elements

The Y2K problem has the potential of affecting any machine that has a microprocessor in it (from microwave transmission facilities to elevators to on-board navigational computers). Performing a survey of these systems was outside the scope of this study. Gartner Group's analysis is focused on the most visible and, in many cases, most critical portion of the technology inventory. Gartner Group identifies below key technology components that are not feasible to take into account as a part of this study, which the Commonwealth will also need to address to achieve statewide Y2K compliance:

- Turnkey process control systems
- Embedded firmware systems
- Telecommunications infrastructure (voice switches, communications controls, radio and satellite systems)
- Facilities infrastructure systems (elevators, environmental controls, security systems, fire control systems)
- Date- and time-aware medical devices (e.g., patient monitoring devices, CAT scanners).

Cost Estimate: Total Cost

Gartner Group estimates that the Commonwealth will spend from $80.2 million (best case scenario) to $83.7 million (worst case scenario) for all Y2K-compliance activities associated with the application portfolio and the underlying computing infrastructure, based on the data supplied by the Commonwealth. These costs are comprised of the following elements:

Technology Area	Cost ($000) Worst Case	Best Case
Applications to be repaired	$31,070	$31,070
Applications to be repaired by contractors	$840.6	$840.6
Applications to be replaced	$8,943	$8,943
Computing infrastructure	$28,889	$28,889
Risk factor	$13,949	$10,461
Total	$83,692	$80,204

5. Findings: Application Compliance

Application Compliance: Introduction

The entire process of achieving Y2K compliance is summarized in Gartner Group's INSPECT (**IN**ventory, **S**cope, **P**arse, **E**xamine, **C**onsider options, **T**actical solutions) methodology. The major steps in the process are described below. The percentages for each stage are based on Gartner Group research regarding the typical portion of time in a Y2K-compliance project that are required for that stage:

- Awareness (1 percent): generating awareness of the Y2K problem.
- Inventory (1 percent): taking an inventory of the systems portfolio, which includes the business function or functions that use an application as well as the application and systems environment.
- Project Scoping (4 percent): obtaining a high-level understanding of the overall project and preliminary compliance unit (CU)—logical groupings of code and (conditionally) data to be upgraded together—segmentation. The sub-projects are identified, estimated and prioritized, with end users involved.
- Examination, Analysis and Solution Design (20 percent): decisions are made per CU regarding logic, data or other compliance approach, producing a customized project plan with detailed resource, duration and risk estimates.
- Modification (20 percent): code modification or package customization, as well as infrastructure and other setup activities.

Application Compliance: Introduction *(Cont'd)*

INSPECT process *(Cont'd)*:

- Unit Test (10 percent): testing of individual programs and the creation of local test scenarios for small groups of programs.
- System Test (25 percent): CU testing, as well as complete regression and logic testing.
- Integration and User Acceptance Test (10 percent): the final testing scenario with user sign-off.
- Implementation, Disaster Recovery and Documentation (9 percent): CUs are moved into production, with facilities for back-out and disaster recovery.
- Project Management: generally is about 25 percent of the total project effort.

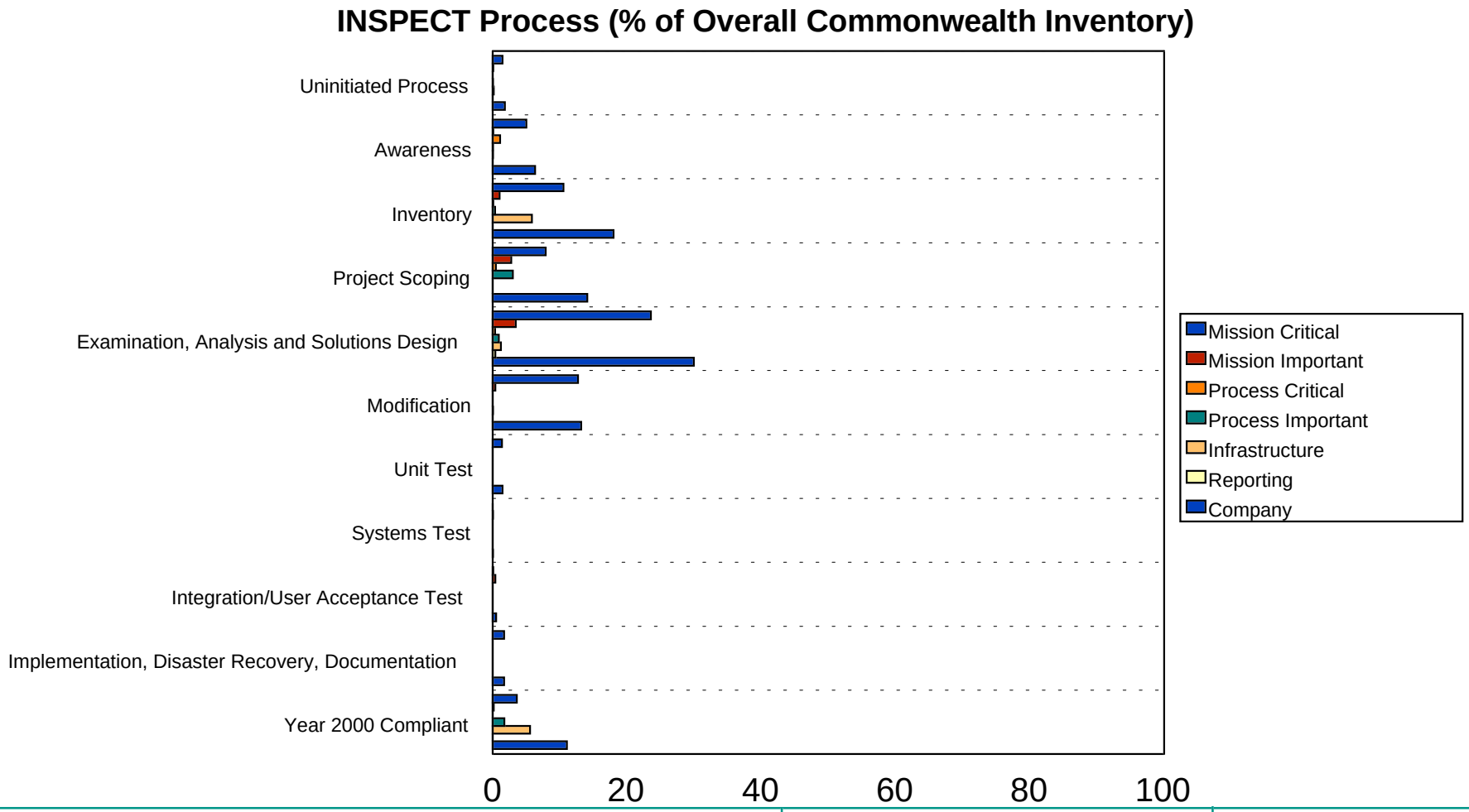
Application Compliance: Degree of INSPECTion

The chart below identifies the position of the Commonwealth's major application categories relative to Gartner Group's INSPECT methodology based on the Commonwealth's self-evaluation. Most applications are in the early stages of the process, with more than 50 percent of the labor effort still to be expended.

	Mission Critical	Mission Important	Process Critical	Process Important	Infrastructure	Reporting	Overall
Uninitiated Process	1.5%	0.1%	0.0%	0.1%	0.2%	0.0%	1.8%
Awareness	5.0%	0.1%	1.1%	0.1%	0.1%	0.0%	6.4%
Inventory	10.6%	1.1%	0.1%	0.4%	5.9%	0.0%	18.0%
Project Scoping	7.9%	2.8%	0.5%	3.0%	0.0%	0.0%	14.1%
Examination, Analysis and Solutions Design	23.6%	3.5%	0.4%	0.9%	1.2%	0.4%	30.0%
Modification	12.7%	0.4%	0.0%	0.0%	0.1%	0.0%	13.2%
Unit Test	1.4%	0.0%	0.0%	0.0%	0.0%	0.0%	1.5%
Systems Test	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.1%
Integration/User Acceptance Test	0.1%	0.4%	0.0%	0.0%	0.0%	0.0%	0.5%
Implementation, Disaster Recovery, Documentation	1.7%	0.0%	0.0%	0.0%	0.0%	0.0%	1.7%
Year 2000 Compliant	3.6%	0.2%	0.0%	1.7%	5.6%	0.0%	11.1%
TOTALS	68.1%	8.5%	2.1%	6.2%	13.0%	0.5%	98.4%

Application Compliance: Degree of INSPECTion *(Cont'd)*

Gartner Group calculated the distribution of the Commonwealth's applications across INSPECT stages, relative to the average percent effort required for each stage. The following chart indicates that the Commonwealth is early in the process.



Application Compliance: Degree of INSPECTion *(Cont'd)*

The total cost to repair by INSPECT stage was assessed, as well as the remaining cost. The chart below shows that the Commonwealth has performed approximately 25 percent of the required remediation effort and that the majority of applications are in the early stages of the process.

INSPECT		Total Cost To Repair	Remaining Cost To Repair
INventory	Awareness	$420,934	$28,158
	Inventory	$420,934	$79,491
Scope	Project Scoping	$1,683,737	$588,662
Parse, Examine, Consider Options	Examination, Analysis, and Solutions Design	$8,418,683	$4,798,791
Tactical Solutions	Modification	$8,418,683	$6,615,112
	Unit Test	$10,523,353	$9,039,716
	Systems Test	$6,314,012	$5,471,248
	Integration/User Test	$2,104,671	$1,829,679
	Implementation/Disaster Recovery/Documentation	$3,788,407	$3,335,672
	TOTAL	$42,093,413	$31,786,529

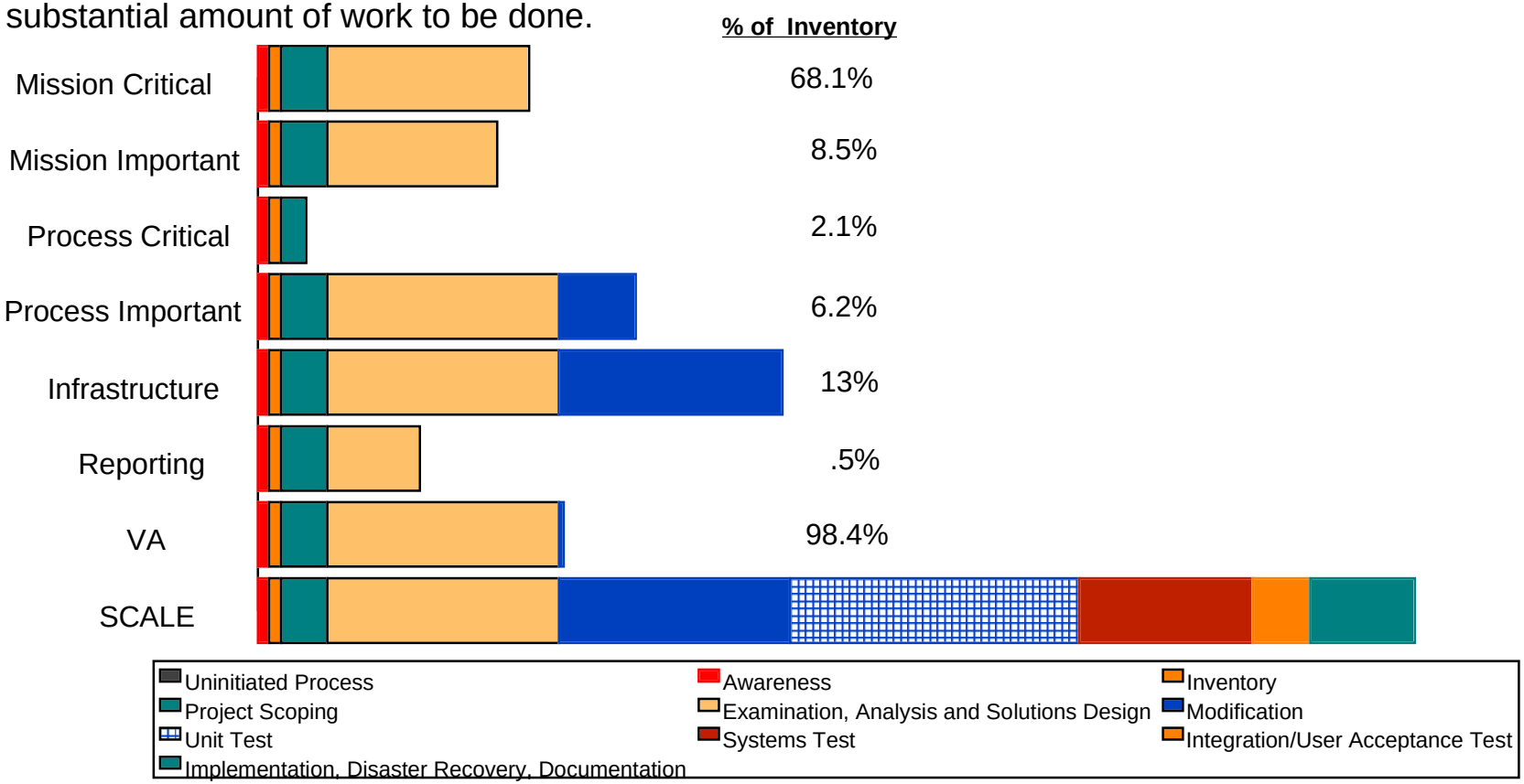
Application Compliance: Degree of INSPECTion *(Cont'd)*

The total and remaining FTE years to repair by stage was determined. The number of personnel that is required can be determined by dividing the total numbers at the bottom by the number of years remaining to completely address the problem (generally less than two years). This number is very high in relation to the Commonwealth's application support staff. The use of external resources will be necessary.

INSPECT		Total FTEs to Repair	Remaining FTEs to Repair
INventory	Awareness	5.4	0.4
	Inventory	5.4	1.0
Scope	Project Scoping	21.6	7.6
Parse, Examine, Consider Options	Examination, Analysis, and Solutions Design	107.9	61.5
Tactical Solutions	Modification	107.9	84.8
	Unit Test	134.9	115.9
	Systems Test	80.9	70.1
	Integration/User Test	27.0	23.5
	Implementation/Disaster Recovery/Documentation	48.6	42.8
	TOTAL	539.7	407.5

Application Compliance: Degree of INSPECTion *(Cont'd)*

The progress indicator represents the expended effort as a percentage of the total amount of effort required to fix the Y2K problem. Details are provided for each system category as well as for the whole organization, with the percentage of the whole inventory for each category listed down the right side. The chart shows that the Commonwealth's efforts to date have been focused on the Process-Important applications and on Infrastructure, which account for 20 percent of the application inventory. However, even these systems are only about 25 percent of the way to achieving full Y2K compliance, which indicates that there is still a substantial amount of work to be done.



Compliance Strategies: Tactical Options

There are a variety of options to make applications Y2K-compliant. These remediation options generally fall into one of the five Rs: repair, replace, reconcile, redeploy and retire. Compliance must be achieved as much in advance of the Time Horizon to Failure (THF), which is the point in time at which an application will fail or produce erroneous results due to a Y2K problem. The THF will vary from one application to another based on the point at which it encounters a date in the next century.

The Commonwealth should plan to make applications Y2K-compliant with an adequate buffer period prior to the THF. This will allow the Commonwealth to determine that the revised application works properly in a production environment.

Each tactical approach is described below:

- Repair: An in-house developed or heavily modified vendor application is revised so as to properly process dates.
- Redeploy: An application is re-written for a new operating platform. The complexities associated with this option are substantial, because both the application and underlying IT infrastructure are changing. This option is typically selected for strategic reasons and in most cases should not be used to fix short-term tactical problems.
- Reconcile: An application is upgraded to a Y2K-compliant version. This approach offers a number of benefits:
  - The Commonwealth is familiar with the vendor and the package, which minimizes risks, time on the learning curve and, possibly, level of effort
  - Some or all costs associated with the upgrade may be covered through existing maintenance agreements
  - The vendor may be willing to provide additional support to significant or long-time customers.

Compliance Strategies: Tactical Options *(Cont'd)*

- Reconcile *(Cont'd)*
  - There are some common issues with this approach that also need to be addressed:
    - » If the package has been significantly customized, the complexity of upgrade may exceed that of a repair option and may also relieve the vendor of maintenance requirements
    - » If the package is not a reasonably current release, the compliance effort will be equivalent to a replace option and may also invalidate vendor maintenance requirements and warranties.
- Replace: An in-house or vendor application is replaced with a Y2K-compliant vendor package (a different vendor if replacing an existing vendor package). This approach may offer the benefits of:
  - Lower maintenance cost of a current vendor package vs. an outdated in-house system
  - Vendor responsibility for bugs and market-driven enhancements
  - Added functionality available in the package product
  - Improved efficiency in operations resulting from the process re-engineering that may accompany package implementation
  - Staff availability for systems that provide a competitive advantage.

  This approach, however, may also require customization to meet the Commonwealth's requirements.
- Retire: An application is discontinued prior to or at the point of Y2K failure. This approach may be used in conjunction with a replacement option or where the cost of achieving Y2K compliance is not economically justified.

Compliance Strategies: Contingency Plans

Contingency for Package Replacement

- The Commonwealth's strategy to replace some Y2K-jeopardized application systems with Y2K-proof packages purchased from reputable vendors is a viable one. The risks involved in a selected revision are manageable. It is essential to carefully plan the rollout of the packaged applications, the timing of data cutover and the timing of systems retirement. In addition, the Commonwealth must provide for the possibility that package implementation will take longer than anticipated or otherwise threaten operations.
- It must be noted, however, that the point for conducting major business process re-engineering while simultaneously trying to achieve Y2K compliance has passed. Strategies for rapid remediation or minimizing business disruption have become paramount. In "ERP and Year 2000 Compliance: BPR Out, Coping In" (KA-345-1361, August 27, 1997), Gartner Group stated that organizations just starting their Y2K analysis problem actually only have nine to 15 months to execute their programs because of the time typically required to complete the THF assessment, determine compliance strategies and gain approval for funding. Replacements from now on must be limited in their scope, and they should be limited to packages with which users already have familiarity.
- To this end, each system slated for replacement must be subjected to risk analysis, prioritization and work effort in the event the old system must be repaired as a precautionary measure.

Compliance Project Phases: Introduction

Planning for Y2K application compliance begins at the end point, which is the THF. The THF is the point in time at which an application will fail or produce erroneous results due to a Y2K problem. The THF will vary from one application to another based on the point at which it encounters a date in the next century. Each compliance strategy will pass through all INSPECT project phases; however, there will be variations that are unique to each strategy. The first three phases of the INSPECT cycle will be similar for all compliance strategies:

- Awareness: Creating awareness of the Y2K problem and gaining commitment will allow the project team to begin assigning the resources in order to solve the problem.
- Inventory: The next step in any compliance strategy is to determine the specific business applications that need to be addressed.
- Project Scoping: This stage becomes the critical first step in determining the likely compliance strategy that will be followed for each application. This is a result, in part, of understanding the resource commitments that need to be made for alternative scenarios.

The unique considerations for each of the remaining phases for each compliance strategy are presented on following pages.

Compliance Project Phases: Repair Characteristics

The repair strategy focuses on detection and correction of date logic and data in existing applications, with other functional modifications as a secondary consideration. The tasks and distribution of effort are consistent with typical maintenance activity, although the level of effort will tend to be higher because of the pervasive nature of date calculations and storage.

- Examination, Analysis and Solution Design: The repair scenario requires a detailed analysis of date logic and data, and provides the widest options for remediation. The level of detail and the variety of options will require a significant investment of time and skilled personnel to be successful.
- Modification: Typically the first step will be to modify the application code, followed by adjusting the stored data, then interfaces to other applications. Successful implementation will depend on a combination of automated tools as well as manual review and changes. It will also be important in the repair scenario to minimize changes involving dates to reduce the complexity of implementation.
- Unit Test: The Commonwealth must develop detailed test scripts to ensure that applications produce consistent (corrected) date results after modification compared to the original functionality.
- System Test: After individual applications are tested, related applications in applications systems must also be tested.
- Integration and User Acceptance Test: The final testing phase should involve both applications maintenance and end-user personnel and should include a period of parallel testing.
- Implementation, Disaster Recovery and Documentation: Applications should be planned for movement into production with a sufficient buffer period before the time horizon to failure.
- Project Management: Will be primarily oriented towards tactical programming and testing efforts.

Compliance Project Phases: Redeploy Characteristics

The redeploy strategy focuses on changing application functionality with Y2K compliance as a secondary, but necessary, consideration. The tasks and distribution of effort are consistent with typical development activity, with some additional effort on setting and monitoring adherence to date-related standards.

- Examination, Analysis and Solution Design: The redeploy scenario focuses on establishing standards for new date logic and storage. Most of the solution design is determined by factors outside the scope of the Y2K problem.
- Modification: The effort in this phase tends to be focused on implementation, not modification.
- Unit Test: The Commonwealth must develop test scripts that test date logic in addition to business functionality.
- System Test: After individual applications are tested, related applications in applications systems must also be tested.
- Integration and User Acceptance Test: The final testing phase should involve both applications maintenance and end-user personnel and should include a period of parallel testing.
- Implementation, Disaster Recovery and Documentation: Applications should be planned for movement into production with a sufficient buffer period before the time horizon to failure.
- Project Management: Will be primarily oriented towards strategic design and functionality testing.

Compliance Project Phases: Reconcile Characteristics

The reconcile strategy focuses on testing Y2K compliance, generally treating the vendor package as a "black box." Efforts for solution design and modification should be minimized, except in cases where there is significant customization of the software.

- Examination, Analysis and Solution Design: The reconcile scenario requires a detailed understanding of each package's date inputs and outputs. The vendor must accept responsibility for an effective solution design.
- Modification: Efforts in this step of the reconcile scenario should primarily be to follow the upgrade instructions provided by the vendor. Addressing the Y2K problem may provide an incentive to eliminate or significantly reduce customization, if any, associated with the non-compliant version.
- Unit Test: The Commonwealth must develop detailed test scripts to ensure that packages are Y2K-compliant, in addition to requiring written vendor assurance of compliance.
- System Test: After individual applications are tested, related applications (packages and/or in-house) in applications systems must also be tested.
- Integration and User Acceptance Test: The final testing phase should involve both applications maintenance and end-user personnel and should include a period of parallel testing.
- Implementation, Disaster Recovery and Documentation: Packages should be planned for movement into production with a sufficient buffer period before the time horizon to failure.
- Project Management: Will be primarily oriented towards vendor interface and package-testing efforts.

Compliance Project Phases: Replace Characteristics

The replace strategy focuses on changing application functionality in addition to addressing Y2K compliance. The tasks and distribution of effort are consistent with typical package implementation activity.

- Examination, Analysis and Solution Design: The replace scenario requires a detailed understanding of the new package's date inputs and outputs as well as overall functionality. The package selection should be based on a vendor's proven solution design.
- Modification: Efforts in this step of the replace scenario should primarily be to follow the upgrade instructions provided by the vendor. Customization should be avoided if possible.
- Unit Test: The Commonwealth must develop detailed test scripts to ensure that packages are Y2K-compliant, in addition to requiring written vendor assurance of compliance.
- System Test: After individual applications are tested, related applications (packages and/or in-house) in applications systems must also be tested.
- Integration and User Acceptance Test: The final testing phase should involve both applications maintenance and end-user personnel and should include a period of parallel testing.
- Implementation, Disaster Recovery and Documentation: Packages should be planned for movement into production with a sufficient buffer period before the time horizon to failure.
- Project Management: Will be primarily oriented towards strategic design and functionality testing.

Compliance Project Phases: Retire Characteristics

The retire strategy focuses on managing the process of eliminating applications while minimizing adverse business impact. The level of activity will be driven by the need to repair as a precautionary measure.

- Examination, Analysis and Solution Design: The retire scenario requires a risk analysis of the impact of eliminating the functionality associated with the targeted application.
- Modification: Efforts in this step of the retire scenario will depend entirely on the level of repair needed to allow the option of extending the useful life of the application, if needed.
- Unit Test: This step will not be necessary for those applications that will definitely be retired.
- System Test: This step will not be necessary for those applications that will definitely be retired.
- Integration and User Acceptance Test: This step will not be necessary for those applications that will definitely be retired.
- Implementation, Disaster Recovery and Documentation: It will be critical to document the rationale behind this strategy as a precaution.
- Project Management: Will be primarily oriented towards setting IT management and end-customer expectations.

Compliance Priority Plan: Introduction

There is a high likelihood that many organizations will not be able to fix the entire application inventory prior to their time horizon to failure date. With this in mind, it becomes essential to prioritize applications to ensure that those with the highest business impact are addressed first. Gartner Group's experience indicates that for most organizations:

- A small number of application systems accounts for the vast majority of overall application functionality (as measured by function points)
- The largest application systems are typically the ones that are the most mission-critical or process-critical
- The largest application systems are generally the least likely to be replaced due to their unique or proprietary nature
- The complexity and difficulty in repairing applications rises exponentially (used in the popular, not the mathematically strict, sense) with size.

As a result, application size becomes a key variable for establishing Y2K-compliance priorities and understanding the associated risk with achieving compliance.

6. Conclusions and Recommendations

Conclusions and Recommendations

Based on the data supplied for this study, the Commonwealth's outstanding cost to achieve Y2K compliance for its IT applications and computing infrastructure will range from $80.2 million (best case scenario) to $83.7 million. The Commonwealth's actual costs will depend on a number of factors which have not been made final at the time of this study, including: determination of the remediation strategy for all applications, the timing and cost of all replacement programs (and whether they can be achieved), the need to repair applications to be replaced or retired and the cost of third-party resources used to augment or replace the Commonwealth staff in the remediation effort. Even during the final data-gathering exercise of this project, Gartner Group found that there were elements of uncertainty about each of these elements. It is worth noting as well that work continues to document the location of all hardware assets of the Commonwealth.

Because of several important factors, the total cost of the Commonwealth's Y2K project is likely to grow beyond this figure. These factors are:

- The Commonwealth's need to rely on external contractors for its remediation and testing work
- The number and magnitude of software packages and hardware platforms not now in the Commonwealth's inventory
- The magnitude of cost required for non-IT assets.

Conclusions and Recommendations *(Cont'd)*

Analysis reveals the following key cost drivers:

- Personnel cost: The total cost of achieving Y2K compliance is calculated using the Commonwealth's fully loaded (compensation, benefits, supporting systems) cost per person. This cost estimate is based upon a fully burdened cost per application support person of $78,000 per year (comprised of compensation, benefits, system and facilities costs). This figure is in line with the average cost for all government units, but it is approximately 29 percent below that of all organizations. It is likely that, as a result of the Commonwealth's broadening of the range of allowable "body shop" relationships and because of the growing demand for qualified resources, the total cost per person of Y2K work will rise toward Gartner Group's average cost level. The cost of the Commonwealth's Y2K project, calculated at this average, would today exceed $115,000,000.
- Size of application portfolio: The Commonwealth's application portfolio is largest in the groupings (government units, database average, eastern U.S. companies and large companies) represented in this study. The current Gartner Group database is comprised of 85 organizations, although Gartner Group has performed approximately 500 application benchmarks since 1990. This positioning is caused by the number and diversity of the Commonwealth's units and their relative homogeneity. As a result, there is relatively little opportunity to create either specialty reuse centers or project management competency center(s). Each group believes that it is in large measure on its own in addressing its Y2K problems. The project has been made that much more complicated by this factor.
- Productivity: Gartner Group's analysis indicates that the Commonwealth's application support productivity is higher than average, but in line with that of government entities in general.

Conclusions and Recommendations *(Cont'd)*

The Y2K problem is matter of survival, not just an IT problem. While the challenges facing the Commonwealth's IT organizations are substantial, the Commonwealth must also begin immediately to address supply chain (suppliers and customers) and non-IT infrastructure issues. As a result, Gartner Group recommends that the Commonwealth:

- Immediately strengthen the central Y2K project office commissioned by the Commonwealth. There must be a core staff of IT and non-IT personnel dedicated to this effort. The project office must leverage the experience of the Commonwealth's Y2K problem "centers of excellence" quickly to disseminate best practices and to leverage tools and techniques. Gartner Group's interviews suggest, for example, that the University of Virginia may be a center of excellence in terms of Y2K planning and organization.
- Empower the project office to set statewide standards and prioritize plans to address the Commonwealth's business applications, IT infrastructure, telecommunications infrastructure, process control systems and supply chain interfaces. These plans must address staffing, service vendor and funding requirements as well as business and IT contingency options.
- Prioritize Y2K compliance efforts. Refine the Commonwealth's application prioritization scheme to ensure that the largest and most business-critical applications are accurately identified. Focus repair efforts on the largest and most critical applications. Gartner Group's analysis indicates that the Commonwealth's Y2K project efforts have been focused primarily on process-important applications and on its infrastructure to date. Progress on mission-critical and mission-important applications is lagging; there is also much work to be done on process-critical applications. The need to redirect focus may well lead to an acceleration of cost.

Conclusions and Recommendations *(Cont'd)*

Gartner Group further recommends that the Commonwealth's Project Management Office:

- Ensure that the Commonwealth monitors compliance progress based on application priority. A critical element of this priority ranking must be the potential legal liability of Y2K failures, particularly in the Department of Corrections and in Medical Assistance Services, and in other areas open to litigation involving entitlements and constitutional rights.
- Establish a Y2K-compliance certification program for the Commonwealth's agencies and institutions and their supply chains.
- Begin an active communication campaign to raise Y2K awareness within the end-user and IT developer communities. Provide guidelines as well as conversion and testing assistance as needed for high-impact systems.
- Extend this communication campaign outside of IT. There was a question among the agencies and institutions interviewed whether there was real focus on the Commonwealth's Y2K problem on the part of decision-makers in state government, particularly in light of the fact that 1997 is an election year.
- Work to develop personnel retention policies and plans, including both financial incentives and targeted management attention. The current plan to provide a cumulative bonus of $10,000 over the balance of the century was deemed insufficient to retain critical personnel. Training commitments can also be used to the Commonwealth's benefit.

Conclusions and Recommendations *(Cont'd)*

The Commonwealth's Project Management Office should also:

- Maintain focus of the Commonwealth's leadership on the Y2K problem and its implications.
  - There were expressions of concern about the amount of incremental unexpected work that would arise as a result of new legislation in the session commencing January 1998. This concern must be analyzed and supported, if appropriate.
  - There was more than one request for a freezing of legislative mandates during the coming session, in order to allow the agencies and institutions to follow through on making the Y2K problem their highest priority. This position must be analyzed and supported, if appropriate.
- Ensure that the Commonwealth's leadership recognizes that the "rules of the game" are changing increasingly rapidly which means:
  - Funding requirements are likely to change over time
  - New service vendor offerings and tools are appearing on a regular basis
  - Ongoing access to current Y2K information, best practices and experts is essential.

Conclusions and Recommendations *(Cont'd)*

- Prioritize Y2K compliance efforts.
  - Refine the Commonwealth's application prioritization scheme to ensure that the largest and most business-critical applications are accurately identified. Develop a composite weighting index, based on the appropriate combination of application size and impact on the functioning of state government. The Commonwealth must be especially aware of the status of applications which entail questions of constitutional rights (e.g., payments of entitlements, offender management).
  - Focus the Commonwealth's repair efforts on the largest and most critical applications first.
    - » Ensure that Commonwealthwide priorities take precedence
    - » Change focus from pilot phase work to implementation
    - » Ensure that adequate staffing is available
    - » Prepare applications services staff for the fact that "success" will not be achieved for a long time due to the size of the applications.
  - Ensure that the Commonwealth monitors compliance progress based on application priority.
    - » Make sure that statewide compliance monitoring and reporting is performed in a priority context
    - » Periodically estimate the Commonwealth's compliance risk based on application priority and functionality.

Conclusions and Recommendations *(Cont'd)*

The Commonwealth's agencies and institutions must:

- Recognize that there are a number of risks associated with package replacement strategies:
  - Qualified implementation vendor resources are becoming increasingly scarce
  - Package implementation may require significant changes to business processes
  - The Commonwealth will need to rely on vendor warranties and reputation to ensure Y2K compliance.
- Understand that the level of package implementation has increased significantly as a result of the popularity of packages and the desire to find a "silver bullet" for Y2K problems. These packages are sufficiently complex to require third party assistance in the implementation process—even when the package may have been imported from another state in which it is already implemented. This increased demand, coupled with the general drain on personnel resources caused by the Y2K problem, has placed a squeeze on qualified implementation vendor resources. The Commonwealth will need to move quickly and get committed vendor resources for those applications to be replaced by packages.
- Appreciate that package implementation requires significant changes to processes. This fact, by itself, creates a risk in any significant implementation effort. This risk is heightened in using packages to solve Y2K issues because it is usually more difficult and time-consuming to change administrative processes than it is to change technical processes. Also, given the short time period until the inevitable millennium change, there can be no back-out plan if the change in business processes is unacceptable or has unintended negative effects. The lack of a "plan B" results in increased risk.

Conclusions and Recommendations *(Cont'd)*

The Commonwealth's agencies and institutions must also:

- Appreciate that the Commonwealth will not be able to test and verify Y2K compliance for all replacement packages. This means that the Commonwealth will need to rely on vendor warranties and reputation to ensure Y2K compliance. The risk is that there could be Y2K-related errors, despite vendor assurances. A potential scenario is that a vendor package fails, resulting in significant business loss to the Commonwealth. However, because all other customers are equally affected, the vendor goes out of business. The Commonwealth's legal protection is, in a practical sense, invalidated because damage rewards are minimal due to vendor insolvency. The principal protection here is selecting the right vendor.
- Understand that the testing phases are particularly time-consuming and demanding of project-management skills. There has been relatively little detailed planning with regard to testing and compliance elements of the Y2K project. These crucial latter stages must be addressed promptly to ensure that the Commonwealth's systems are fully compliant. Furthermore, the Commonwealth's agencies and institutions must be aware of their need to conduct testing on midrange platforms.

Conclusions and Recommendations *(Cont'd)*

- There are several additional elements worth mentioning.
- While the Commonwealth has been able to make Y2K-compliance certification a requirement for software acquisitions, this requirement must be enforced in all other technology procurements as well, effective immediately.
  - Procurement standards should specifically address:
    - » Application packages (date storage, logic and interfaces)
    - » IT infrastructure (hardware, firmware, operating systems, major subsystems, utilities)
    - » Telecommunications infrastructure (routers, hubs, switches, PABXs, transmission facilities, satellites, ACDs, VRUs, etc.)
    - » Process control systems (integrated control systems, logic chips, monitors, process control microprocessors, etc.).
  - Known Y2K problems do exist and should be taken into account in any procurement:
    - » Personal computers. Some sources indicate that at least one-quarter of personal computers currently being sold are not Y2K-compliant. Problems may be the result of issues with the hardware, BIOS and/or interface cards.

Conclusions and Recommendations *(Cont'd)*

Generally, the Commonwealth should be careful when comparing its results to those of other states, keeping the following points in mind:

- Different states are at different points in dealing with the problem.
- The results reported by each state must be normalized based on the size and nature of the application inventory as well as the size of the state.
- The methodology used to develop the other estimates must be understood, since other states may have internally underestimated the cost to address the Y2K problem fully.

Appendix A:
Interview Participants

Interviews: Participants

The persons identified below were interviewed individually or in small groups by Gartner Group. They were recommended by JLARC staff. The names are presented alphabetically by business unit and sequence is intended only for ease of reference.

Business Unit	Name	Title	Date
Accounts	Deborah Johnson	Director, Information Resources	Jul 17, 1997
Accounts	Jeff Smith	Year 2000 Project Coordinator, System Analyst	Jul 17, 1997
Accounts	Richard Salkeld	Manager of Systems and Projects	Jul 17, 1997
Accounts	Robert Meinhard	Financial Analyst	Jul 17, 1997
Corrections	Larry Troemmler	Contingency Planning Manager	Jul 16, 1997
Council on Information Management	Bette Dillehay	Data Administrator	Aug 26, 1997
Information Technology	Bob Collier	Manager, Information Systems Development	Jul 16, 1997
Information Technology	Wayne Robertson	Director, Management Information Systems Division	Jul 16, 1997
Information Technology, SDD	Dale Kurowsky	Information Technology Manager	Jul 17, 1997
Medical Assistance Services	Bill Burnett	Systems Analyst, Information Management Division	Jul 17, 1997
Medical Assistance Services	Bob Clewell		Jul 17, 1997
Medical Assistance Services	John Orrock	Senior Database Administrator, Information Management Division	Jul 17, 1997
Retirement Systems	Sharon Perdue	IS Manager	Jul 17, 1997
Social Services	Lewis Clark		Jul 16, 1997
Taxation	HF Jones	Applications Manager, Office of Information Resource Management	Jul 16, 1997
University of Virginia	Bernie Hill	Development Manager	Aug 28, 1997

Appendix B:
Agency and Institution Information

Agency and Institution Detail: Percentage of Completion Estimates

Based on Gartner Group estimates, the Commonwealth has expended varying amounts of the effort required to make all IT applications Y2K-compliant. The table below presents the specifics for the twenty largest applications in the Commonwealth's application set.

Agency Name	Application Description	Compliance Strategy	Completion Percent	Function Points	Function Percent
Info Tech Division	BUREAU OF INSURANCE	Repair	1.5%	33,853	5%
Department of Transportation	HIGHWAY TRAFFIC RECORDS	Repair	1.5%	30,249	4%
Dept. of Mental Health / Substance Abuse	HUMAN RESOURCES INFORMATION SYSTEM	Compliant	100.0%	28,580	4%
Dept. of Mental Health / Substance Abuse	PATIENT/RESIDENT AUTOMATED INFO SYSTEM	Repair	36.0%	27,618	4%
DMV	CITIZEN SERVICE SYSTEM	Repair	16.0%	27,469	4%
Taxation	STATE TAX ACCOUNTING & REPORTING SYSTEM	Repair	0.5%	26,571	4%
William & Mary College	STUDENT INFORMATION	Repair	36.0%	25,607	4%
Lottery	BACK OFFICE SYSTEM	Repair	1.5%	18,000	3%
Department of Transportation	FINANCIAL MANAGEMENT SYSTEM - 501	Repair	1.5%	15,096	2%
Dept. of Medical Assistance	VA MEDICAID MGMT INFO SYSTEM	Repair	16.0%	13,956	2%
University of Virginia	INTEGRATED STUDENT INFORMATION SYSTEM	Repair	36.0%	11,881	2%
Lottery	ONLINE GAMING SYSTEM	Repair	95.5%	11,863	2%
Virginia Community College	STUDENT INFORMATION SYSTEM	Repair	16.0%	11,738	2%
DIT	TELECOMMUNCATIONS INVENTORY BILLING FORM	Repair	4.0%	11,256	2%
Virginia Tech	STUDENT - REGISTRAR	Repair	16.0%	10,999	2%
DSS	STATE VERIFICATION AND EXCHANGE SYSTEM	Repair	58.5%	10,106	1%
University of Virginia	EMPLOYMENT SYSTEM	Repair	4.0%	9,520	1%
DMV	CUSTOMER SERVICE CENTER NETWORK	Repair	100.0%	9,435	1%
OCCS	INSTITUTIONAL ADVANCEMENT SYSTEM	Repair	100.0%	9,287	1%
OCCS	INTEGRATED STUDENT INFO SYSTEM	Repair	16.0%	9,154	1%
COMMONWEALTH TOTAL			26.0%	711,806	100%

Agency and Institution Detail: Cost Estimates

The information presented below identifies the cost of total and remaining repair efforts for each agency and institution of the Commonwealth. It does not include the cost of replacement efforts, or of hardware remediation efforts. The numbers reported reflect those supplied by the Commonwealth's agencies and institutions to Gartner Group.

Agency Name	Total Cost	Remaining Cost	Agency Name	Total Cost	Remaining Cost
Alcoholic Beverage Control	$ 95,974	$ 57,292	Info Tech Division	$ 2,778,985	$ 2,715,742
Department of Corrections	$ 473,954	$ 347,297	James Madison University	$ 545,266	$ 464,713
Department of Health	$ 80,570	$ 9,266	Lottery	$ 1,765,980	$ 1,080,051
Department of Juvenile Justice	$ 36,960	$ -	OCCS	$ 1,942,517	$ 1,244,134
Department of Transportation	$ 3,682,792	$ 3,247,241	Retirement Systems	$ 701,936	$ 592,652
Dept. of Accounts	$ 551,320	$ 368,028	State Police	$ 1,074,368	$ 903,427
Dept. of Medical Assistance	$ 1,910,519	$ 1,615,106	Supreme Court	$ 1,957,466	$ 1,360,301
Dept. of Mental Health / Substance Abuse	$ 4,296,042	$ 1,486,914	Taxation	$ 2,091,022	$ 2,075,370
Dept. of Social Services	$ 2,107,105	$ 1,252,586	University of Virginia	$ 3,623,220	$ 3,220,162
DIT	$ 1,674,877	$ 1,607,881	UVA Medical Center	$ 82,105	$ 50,434
DLAS	$ 145,336	$ 8,826	Virginia Commonwealth	$ 384,242	$ 253,141
DMV	$ 2,571,181	$ 1,686,947	Virginia Community College	$ 830,952	$ 697,999
Employment Commission	$ 1,779,821	$ 1,374,646	Virginia Tech	$ 2,810,430	$ 1,896,292
George Mason University	$ 495,837	$ 416,503	William & Mary College	$ 1,514,307	$ 959,156

Agency and Institution Detail: Personnel Risk Indicators

Gartner Group identified certain risk indicators associated with committed staffing levels and organizational stability (note: risk areas are flagged as "XXX"). The table below presents the specifics for each business unit.

Agency	Low Tenure *(average less than 3 yrs)*	Staff Shortage *(50+% staff needed for repair)*	Staff Turnover *(25+% recent staff turnover)*
Accounts		xxx	
Alcoholic Beverage Control		xxx	xxx
College of William and Mary			
Community College System		xxx	
Corrections		xxx	xxx
Elections		xxx	
Employment Commission		xxx	
George Mason University		xxx	
Information Technology			
James Madison University			
Juvenile Justice		xxx	
Legislative Automated Systems			
Lottery			xxx
Medical Assistance Services		xxx	xxx
Mental Health, Mental Retardation and Substance Abuse			
Motor Vehicles			
Old Dominion University OCCS			xxx
Retirement Systems			
Social Services			
State Police		xxx	
State Corporation Commission	xxx	xxx	
Supreme Court			
Taxation		xxx	xxx
Transportation			
UVA Medical Center			
University of Virginia			xxx
Virginia Commonwealth University		xxx	xxx
Virginia Tech		xxx	
TOTAL NUMBER (%) OF AGENCIES	1 (3.60%)	14 (50.00%)	8 (28.57%)

Appendix C: Competing Initiatives

Agency and Institution Detail: Competing Initiatives, 1997 – 2000

Agency	Total Available Labor Pool	Planned Y2K FTEs	Planned New Initiatives 1997 – 2000 (not in priority ranking)
Accounts	12	10.3	Data warehouse conversion from Adabas to Oracle Integrated human resources information system Upgrade PCs to Win 95 / Office 97 Upgrades to vendor software
Alcoholic Beverage Control		15	New enforcement system New financial management system New product distribution system Upgrade to LAN / WAN
College of William and Mary	11	5	BPR projects in personnel and payroll Data warehouse DB2 version upgrade Develop preventive maintenance system Expansion of Web-based delivery of information on campus Financial records system version upgrade HR system version upgrade Install mainframe tape management system Mainframe OS and CICS upgrade Reengineer campus police incident-based reporting system Reengineer student housing, student billing / receivables and transcript systems Software AG product suite version upgrade

Agency and Institution Detail: Competing Initiatives, 1997 – 2000 *(Cont'd)*

Agency	Total Available Labor Pool	Planned Y2K FTEs	Planned New Initiatives 1997 – 2000 (not in priority ranking)
Community College System	8	11	SIS fee enhancements SIS replacement systems (MF to GS)
Corrections			Offender management system (replacement of 90% of existing systems)
Employment Commission	27	20	Common intake implementation Conversion from microfilm to COLD Local office image expansion New LAN / WAN One Stop: LMI access; America's Job Bank; America's Talent Bank Tax image
George Mason University	53	20	Acquire / implement Oracle information retrieval system Upgrade / replace mainframe to enhance performance
Information Technology	6	4	Conversion of telecommunications system to Oracle Implementation of new version of supplied financial systems Implementation of Oracle Web server Komand upgrade Miscellaneous billing systems Place personnel system on DIT's intranet Telecommunications budget and resource forecasting system

Agency and Institution Detail: Competing Initiatives, 1997 – 2000 *(Cont'd)*

Agency	Total Available Labor Pool	Planned Y2K FTEs	Planned New Initiatives 1997 – 2000 (not in priority ranking)
James Madison University	42	2	Capacity upgrade of campus network Computerized maintenance management system (CMMS) Development of enhanced Web services OS upgrades on servers and PCs: move to NT server, Win NT, and HP-UX Possible transition of University Advancement system to new hardware and software Upgrade (potential rewrite) of bookstore management system Upgrade of campus telephone system Upgrade of circulation and library management system Upgrade of security system
Juvenile Justice	1	1 (part-time)	Implementation of new RS/6000 automation server Juvenile tracking system expansion Migration to new desktop from Windows 3.1x Office automation expansion OS upgrade on all RS/6000 servers Public safety data collection and sharing effort
Legislative Automated Systems	18	0.5	Implementation of NT server LIS (mainframe to client/server) Upgrade PCs to Win 95 and Win NT

Agency and Institution Detail: Competing Initiatives, 1997 – 2000 *(Cont'd)*

Agency	Total Available Labor Pool	Planned Y2K FTEs	Planned New Initiatives 1997 – 2000 (not in priority ranking)
Lottery	12	10 contract staff	Big Game enhancements Cash option for Lotto / Big Game Full redemption
Medical Assistance Services			MMIS replacement project Upgrade of LAN operating system Upgrade to Oracle Financials v10.7
Mental Health, Mental Retardation and Substance Abuse	17	1	FMS upgrade HP3000 upgrade
Motor Vehicles	1795	25	DMV Internet project Elien enhancements Mandated legislative changes National motor vehicle titling (NMVTIS) Natural 2.3 upgrade PC upgrades Series / 1 replacement project: CSCNET (UNIX platform) VM system replacement

Agency and Institution Detail: Competing Initiatives, 1997 – 2000 *(Cont'd)*

Agency	Total Available Labor Pool	Planned Y2K FTEs	Planned New Initiatives 1997 – 2000 (not in priority ranking)
Old Dominion University OCCS	12	4.5	Administrative systems replacement Client/Server development—Web-based development Communications enhancement—ATM network Data warehouse Infrastructure upgrades—consolidation of voice, video and data services Infrastructure upgrades—Web-based instruction Lotus Notes deployment NT deployment Re-hosting of VM supported services
Retirement Systems	11	6	Employee bulletin board installation IVR installation Possible rewrites of disability and refund systems Win 95 installation
Social Services	138	5	ADAPT Data warehousing Day Care Financial systems SACWIS

Agency and Institution Detail: Competing Initiatives, 1997 – 2000 *(Cont'd)*

Agency	Total Available Labor Pool	Planned Y2K FTEs	Planned New Initiatives 1997 – 2000 (not in priority ranking)
State Police	12	102 man months	CAD/MCT implementation statewide Communications upgrade Criminal history records improvement project Incident-based UCR (SCRIBE) implementation Integrated criminal justice information system (ICJIS) implementation Interface of IAFIS with federal system Migration to Office 97 NCIC-2000 interface with FBI Rollout of evidence management system Statewide implementation of new composite system TIPS system phase III implementation Upgrade of mainframe to ClearPath
State Corporation Commission	40	10	Redesign of Clerk's information system Replacement of financial management system, CASE management system Upgrade of desktop software, operating systems and database software
Supreme Court	13	5	24 special projects outlined for 1997 – 1998 alone

Agency and Institution Detail: Competing Initiatives, 1997 – 2000 *(Cont'd)*

Agency	Total Available Labor Pool	Planned Y2K FTEs	Planned New Initiatives 1997 – 2000 (not in priority ranking)
Taxation	52	n / a	Public / private partnership system: Planned complete replacement
Transportation	57	15	Bid analysis management and construction management system Bridge management system Data warehouse Financial management system Geographic information system Integrated document management system Integrated human resources information system Integrated maintenance management system Pavement management system Right-of-way and utilities management system Traffic monitoring system Virginia operations information system
UVA Medical Center	50	8	72 initiatives outlined for 1997 – 2000

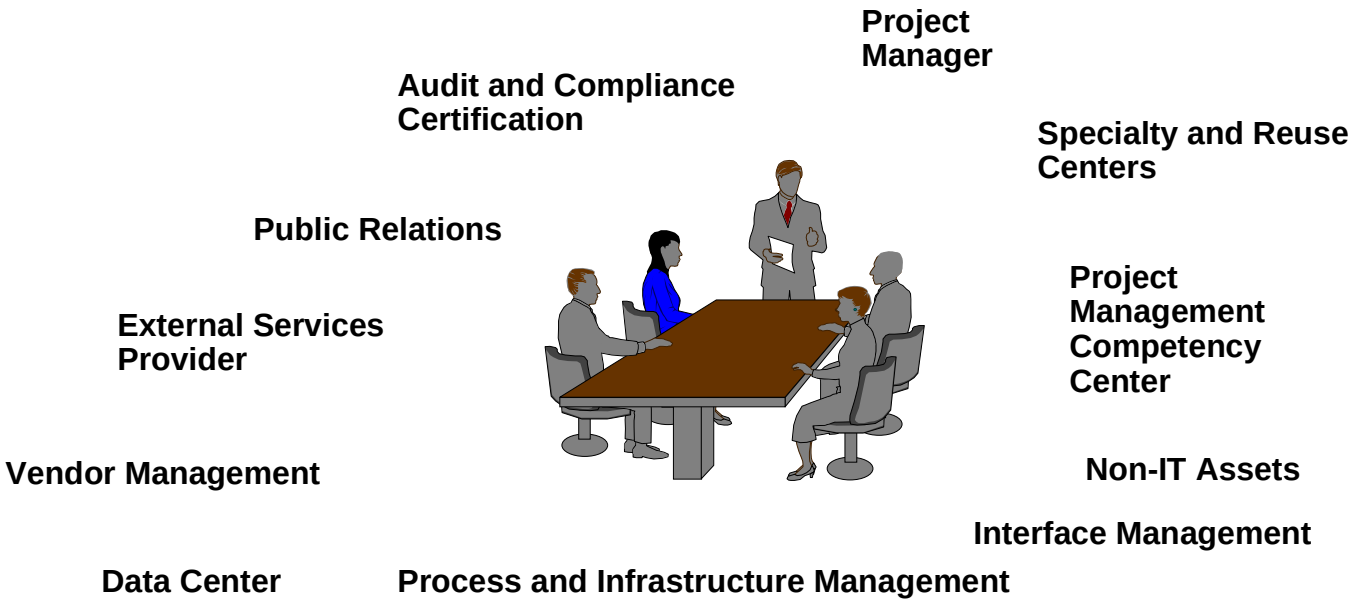
Agency and Institution Detail: Competing Initiatives, 1997 – 2000 *(Cont'd)*

Agency	Total Available Labor Pool	Planned Y2K FTEs	Planned New Initiatives 1997 – 2000 (not in priority ranking)
University of Virginia		23	Implementation of Universitywide payroll/ personnel system Installation of ATM OC-12 network Replacement of at least 1 legacy administrative system Replacement of existing mainframe with enterprise server Upgrade of UNIX machines
Virginia Commonwealth University		16	Replacement of current student information system with vendor system Upgrade of existing financial and HR systems Upgrade of existing NOTIS library system
Virginia Tech	5800 FTEs	43.5	Digital server upgrade Implementation of Citrix Systems infrastructure tool Mainframe hardware/OS upgrades Mainframe to client/server migration of finance and student systems Mainframe to client/server migration of HRIS, alumni development systems

Appendix D: Personnel Management Supplemental Information

Project Management: Year 2000 Project Office

Gartner Group generally recommends the creation of a Year 2000 Project Office which would have authority over needed resources. The Project Office would generally include the functions shown below. One component, a Project Management Competency Center (PMCC), would support individual project managers and provide services such as project plan templates and estimating models.



Personnel Management: Retention

The potential for loss of key applications personnel is substantial (Gartner Group research indicates that personnel movement may be up to four times larger than current IT industry averages). Because of the enormous worldwide labor requirements needed to address the Y2K problem, the Commonwealth is probably at risk from aggressive poachers from other companies, including external service providers. Gartner Group suggests the following strategies:

- Recognition from Commonwealth leadership of the critical role of the Y2K team ensuring that the Commonwealth's IT infrastructure continue to function.
- Elevation of Y2K team members to an esteemed status, possibly including premium wages.
- "Stay Bonuses": Significant cash incentives to staff who remain until Y2K remediation is complete.
- Retraining in new skills promised to staff following the Y2K commitment.

Personnel Management: Project Team Requirements

Year 2000 project teams have certain requirements to maximize project success. These include:

- Skills
  - Project Managers: Skilled project managers are scant due to high demand and are essential for Y2K project success. This is true for both large-scale package replacement implementation and repair projects. In-house expertise is preferable, but contractors should be brought in if sufficient in-house skills are lacking.
  - Programmers: Structured analysis and programming skills, primarily in legacy languages such as COBOL, are essential to quickly and accurately solving the Y2K problem. Programmers will also generally need to become adept at using date detection and/or correction tools that are selected as part of the Commonwealth's Y2K toolkit. It will be a challenge to find the right balance of tasks to keep the best programmers motivated throughout the long process of maintaining and fixing code.
  - Testers: Dedicated test teams must be created for the crucial task of verifying and validating Y2K-compliant code. Test personnel will need to ensure that non-date-related functionality is not compromised by date-related changes.
- Training
  - The Commonwealth should provide either internal or external training in needed skills, e.g., project management, remediation methodologies and tools.

Personnel Management: Communication Program

Any activities that the Commonwealth initiates to promote the importance of the Y2K project will assist in successfully addressing the full scope of enterprise issues associated with the problem. Ideas include:

- A Y2K newsletter detailing the progress of the project at the Commonwealth and disseminating ideas and news on the topic from the Internet and other industry sources
- A Y2K suggestion box where Commonwealth employees can post their ideas; this could be tied to some kind of recognition and reward program or contest
- A Y2K bug box where Commonwealth employees can identify problems and potential solutions
- A Y2K groupware database (for example in Lotus Notes or Exchange) as an electronic forum for sharing issues and solutions, as well as a tool for communicating progress in achieving Y2K compliance
- An intranet location for storing Y2K policies, procedures and tools
- Posters and agency Y2K logos will help to keep the project visible
- Periodic E-mail notifications.

Appendix E: Compliance Testing Supplemental Information

Testing: Overview

Testing is a critical component of any application service, including development, maintenance and package implementation. The goal is to minimize the likelihood that applications will fail or, just as important, produce erroneous results, as a result of incorrect data input or processing. The testing component of Y2K projects will be more difficult than that of other software projects due to the following:

- The scope of the testing effort is enormous. The majority of the Commonwealth's applications (in-house-developed as well as third-party) must be tested. All application code and data definitions must be analyzed and tested, since date-based processing could impact up to 40 to 50 percent of the functionality of many systems. Consequently, testing requirements will be greater than under normal scenarios. The complexity of the test requirements will be further increased in situations where changes are made at the same time that are not related to date handling in addition to those that are related.
- All levels of the computing infrastructure are affected. The problem can be resident in hardware, firmware, machine-level software, operating system software, sub-system software and application software. The implications of this are quite significant in that different Commonwealth groups as well as third parties are typically responsible for each level; however, all must be Y2K-compliant for end-user applications to operate correctly.
- Time is the enemy. All Y2K remediation efforts must be completed in a relatively short time frame. Typically, the time for integration and implementation testing is restricted to non-critical periods (like weekends) which significantly reduces the time window available for testing. This time compression may also lead to scarcity of another resource: IT and end-user personnel available to perform the testing.

Testing: Planning

A carefully designed test plan must be created to mitigate the risks associated with the Y2K problem. Some considerations include:

- Methodology: The first step in planning is to determine an overall methodology. There are three conceptual approaches: 1) top-down or logical, 2) bottom-up or physical, or 3) a combination approach. The latter approach may reduce the Commonwealth's overall Y2K testing costs.
- Test Bed: It is essential that testing does not disrupt "business as usual" operations. There are a number of ways to establish a test bed, i.e., a testing environment that is compartmentalized from the production environment to prevent "contamination" of the current operational environment. Options include:
  - Physical partitioning—establish a separate, duplicate environment for testing purposes. This is the most foolproof and expensive option.
  - Logical partitioning—segment the current physical environment into separate areas for testing purposes. Usually logical partitions are variable in configuration and the implementation and level of security varies from one technology platform to the next.
  - Time partitioning—separate usage for test from production purposes based on time of day and/or day of week. This is the riskiest, but least expensive, option.
- Test Cases: The Commonwealth must establish a baseline of test data in the early in the Y2K project. The amount of test data will depend upon the number of compliance units that must be certified, user acceptance criteria and defined coverage requirements.

Testing: Planning *(Cont'd)*

- Testing Tools: A test toolkit is an essential component of a test plan. See vendors and tools section for additional information.
- Capacity Considerations
  - CPU (processor) capacity should be estimated using standard techniques. If possible, this approach will maintain the integrity of the testing environment (e.g., simulated dates, test programs and data) and minimize the impact on the existing production environment. Additional CPU capacity may not be needed if testing can be scheduled during off-peak periods or low-priority applications can be deferred into low utilization periods.
  - DASD (disk space) capacity needed will depend on the size of the regression test bed, which will be based on coverage requirements. It is expected that additional disk storage will be needed to satisfy testing requirements. Due to the short time horizon for this need, these requirements can be addressed through short-term leases.
- Quality Assurance (QA)
  - QA steps, such as inspections and specific test methods, should be an integral part of the Y2K project plan. Training is an integral part of the QA process.

Testing: Certification

Every key application must be tested for Y2K compliance. An audit process should be used to demonstrate that date manipulations and the resulting calculations are correct when the century boundary is crossed.

Sample certification criteria for the various layers of an application are:

- User layer: User interfaces and reports must account for the century in a manner acceptable to end users, including:
  - four-digit year display and data entry fields (or user acceptance of proper two-digit year)
  - correct date sorts
- Logic layer: Proof of correct date routine logic or demonstration that date processing is routed through a common Y2K-compliant subroutine
- Interface layer: Demonstration that dates passed through point-to-point interfaces or EDI transactions are correct:
  - identification of all interface points
  - proof of correct date format and value passing
  - proof of effectiveness of any filters used as protection
  - proof of compliance from all interface partners
- Data layer: Identification of all data access points and proof of Y2K-compliant data fields

Testing: Certification *(Cont'd)*

Third-party software: Gartner Group recommends that the Commonwealth obtain certification from software vendors similar to the following:

- "The licenser warrants that the software, which is licensed to licensee hereunder and used by licensee prior to, during or after the calendar year 2000, includes or shall include, at no added cost to licensee, design and performance so the licensee shall not experience software abnormally ending and/or invalid and/or incorrect results from the software in the operation of the business of the licensee. The software design to ensure Y2K compatibility shall include, but not be limited to, date data century recognition, calculations that accommodate same century and multi-century formulas and date values, and date data interface values that reflect the century."

Following are representative definitions of Y2K compliance:

- "The capability of a Product, when used in accordance with its associated documentation, to correctly process, provide and/or receive date data within and between the 20th and 21st centuries, provided that all other products (for example, hardware, software, and firmware) used with the Product, properly exchange accurate date data with it." (*IBM*)
- "A product certified as being Year 2000 compliant will not produce errors in date data related to the year change from December 31,1999 to January 1, 2000 and date representation by the product will be accurate into the future, until the year 2037. The compliant product will define specific, non ambiguous representation, handling and interpretation of centuries represented by two digits." (*SunSoft)*

Testing: Certification *(Cont'd)*

Definitions of Y2K-Compliance (*Cont'd*)

- "The software must perform fault-free in the processing of date and date related data (including, but not limited to, calculating, comparing, and sequencing) by all hardware and software products delivered under this contract/procurement, individually and in combination, upon installation. Fault-free performance includes the manipulation of this data with dates prior to, through, and beyond January 1, 2000, and shall be transparent to the user. Hardware and software products, individually and in combination, shall successfully transition into the year 2000 with the correct system date, without human intervention, including leap year calculations. Hardware and software products, individually and in combination, shall also provide correct results when moving forward or backward in time across the year 2000." *(General Services Administration recommendation for mandatory technical specifications for computer hardware, software and services acquisitions)*

Testing: Phases

Test planning and execution must ensure delivery of high-quality components that are Y2K-compliant. Testing must start with the year of modification and extend through 2001. Compliant applications must then be put into production, including data migration and provisions for rollback as needed.

Phase	Key Deliverable
• Test Planning	Test plan
– Define scope, requirements to be verified	
– Define related acceptance and completion criteria	
– Define tools, techniques and resources to be used	
– Define schedule	
• Test Case Design	Suite of documented test cases
– Design cases that verify application requirements	
– Define cases that perform user interface verification	

Testing: Phases *(Cont'd)*

Phase	Key Deliverable
• Test Development – Transform test cases into reusable test scripts – Create test data, e.g., via capture-playback simulators	Suite of test scripts and test data
• Test Execution and Evaluation – Utilize test scripts – Evaluate results against baseline – Determine if requirements have been met	Series of verification reports

Appendix F: Tools and Vendors Supplemental Information

Toolset Options

Tools can help in all phases of the Y2K project: awareness, inventory, detection, documentation, repair, software distribution and change implementation. Exploiting tools throughout the compliance project can yield overall savings while providing a more robust infrastructure for change.

Leveraging Tools

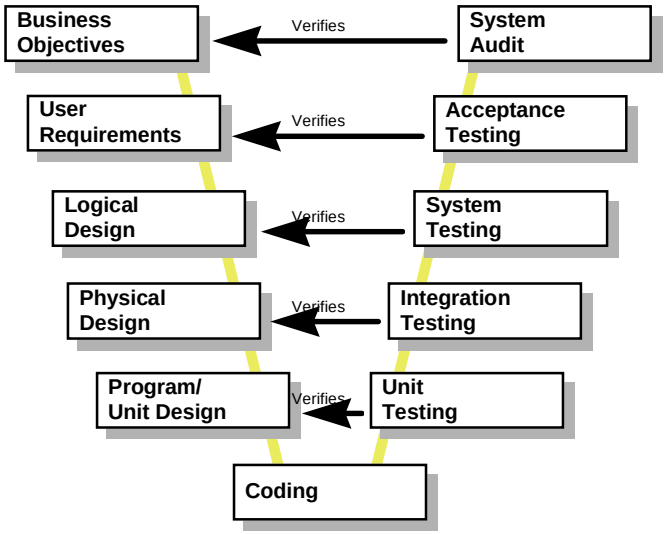
- By conducting an inventory of tools currently in use before deciding to acquire new tools for the year 2000, the Commonwealth can leverage its existing contracts, customized implementations and skill sets.

Methodologies

- The Commonwealth should adopt a single development methodology that contains a software quality and testing thread in each and every project phase.
  - For example, during application requirements definition, certain performance and service-level criteria should be specified in the test plan (e.g., the application must support dates prior to, during and after 2000). These criteria then feed test case development with the requirement to execute the three date scenarios. Similarly, additional test cases are created during application analysis and design. During application code construction, reusable test scripts and beds of test data are generated. Finally, during application testing, test scripts are executed and results are analyzed. This is an example of the “V-test” methodology, in which AD and testing activities eventually join at the bottom of the V during the traditional testing phase.

Toolset Options *(Cont'd)*

V-test Methodology



"V-Test" Explanation

The "V-Test" principle is a public domain, test methodology framework. It depicts testing as stages of verification, with the coding effort residing at the bottom of the "V." The left side (arm) of the "V," from top to bottom, represents the traditional applications development (AD) life cycle stages. The right side (arm) represents the corresponding test phases, which seek to verify the key deliverables of the AD life cycle. From a testing perspective, begin at the top, left hand side of the "V" and conduct a series of static tests where the application under test is not exercised (e.g., reviews, inspections, walk-through sessions and desk checks). Just after the coding phase, testing then becomes dynamic and proceeds up the right arm of the "V," finishing at the top. Dynamic testing exercises the application or its components with test scripts. It must pass through "quality gates" (i.e., approvals of key test/verification deliverables) before moving from one stage to the next.

Parsing and Conversion

- Conversion tools are either passive (only annotates what to change); active (annotates and may perform changes); or software factory (an off-site lab where code is analyzed based on parsing rules and changes are applied). All results must be verified. Key decision factors are scale, language, platform and the standardization of date routines.
- Where applicable, the Commonwealth's common modules that handle date routines should be inventoried, analyzed, modified and tested. Some programs will have "hard-coded" date manipulations which need to be identified and fixed.

Toolset Options *(Cont'd)*

Standards

- The Commonwealth should promulgate a set of standards and "best practices" which are followed by all staff, whether or not specifically involved in the Y2K project.
  - Every user and application developer who reviews or modifies an existing program should be trained to check for Y2K compliance and (at a minimum) note irregularities and (if feasible) make the appropriate changes.
  - Proper date-handling practices must be taught to all user and application developers so that the Y2K error is not built into new applications. Application review processes should be in place to identify invalid use of dates and procedures for correcting such errors.
- Change Management
  - The need for effective change management will be critical throughout the Y2K-compliance project life cycle. The Commonwealth should review its existing change management tools to determine their ability to assist in this endeavor.

Toolset Options: Toolkit

Components of a Y2K testing toolkit include:

- Debuggers: Finds errors in program logic
- Date Simulators: Intercepts and simulate system date and time calls for Y2K test situations
- Test Planning and Management: Helps plan, build, execute, analyze, manage and report on results of test cases and scripts
- Capture and Playback: Performs automated regression testing, captures keystrokes and results to create a baseline (regression test bed) against which generated test scripts can be measured
- File and Data Manipulation; Test Data Generation: Facilitates extracting, reformatting, customizing and loading of test data
- Software Change Management: Automates rules for ensuring low-risk change throughout the Y2K project
- Problem Management and Tracking: Captures, analyzes and manages problem resolution.

Defect prevention and removal processes:

- JAD (joint application development) and prototyping are especially effective for ensuring high levels of functional quality due to the involvement of end users
- Inspections are the most effective means of removing most project defects. Done early, inspections reduce testing time
- Regression testing tools will facilitate the system and acceptance phases of the Y2K project.

Vendors

The Commonwealth must institute procedures to guard against possible re-infection from the non-Y2K-compliant data of customers, suppliers and vendors. Some options include:

- Contact interface partners and agree on a schedule for implementing new date formats
- Obtain warranty or certification of Y2K compliance, especially from mission-critical upstream partners and suppliers
- Where appropriate, build filters and/or firewalls to protect against infected data.

Vendors: Application Vendors and Technologies

- All of the Commonwealth's third-party application software vendors, followed by systems software vendors, should be contacted about the status of their products' Y2K compliance.
- In addition to obtaining written vendor assurances, the Commonwealth must test each package as part of its overall test plan, both to ensure compliance and to understand that the method of obtaining compliance is accommodated by the Commonwealth's systems.
- If Y2K compliance will be provided in a future release and the Commonwealth's version is up to date, the compliant version will probably be provided free. The Commonwealth should schedule the upgrade to provide an orderly migration with appropriate testing.
- If the Commonwealth's version is sufficient releases behind, maintenance contracts must be reviewed, and in-house customizations evaluated, to estimate the cost and desirability of upgrading vs. switching to another product.
- If the vendor's response (or lack of one) casts doubt on its Y2K compliance, the Commonwealth's options are to move to a competitor's product, get access to the source code, or institute legal actions.